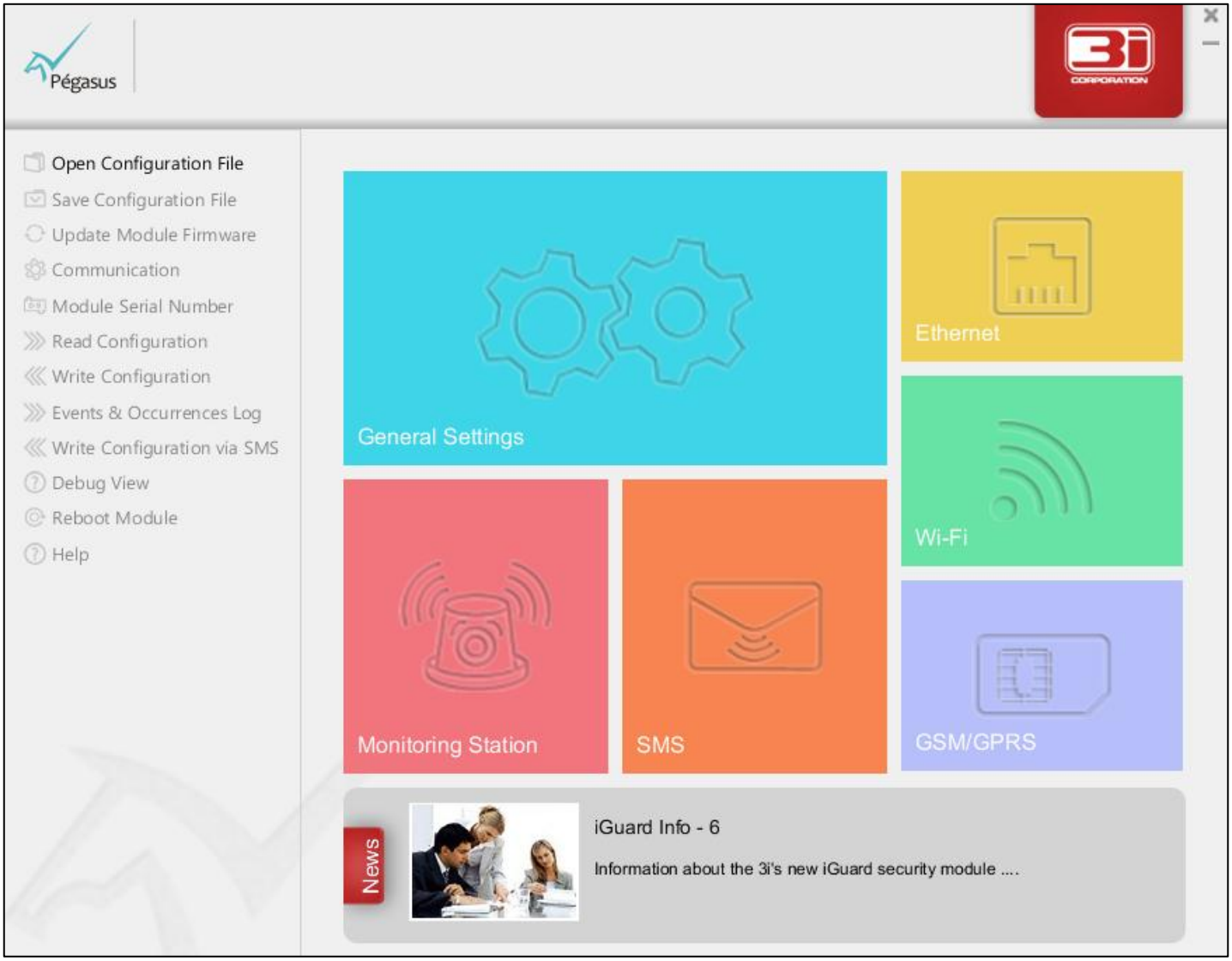
User Manual

Pégasus™

Studio



Pegasus™ Studio – Configuration Tool

User Manual | April 2013

3i Technology Solutions Pvt. Ltd.

No. 5, 1st Floor, Khykha Court, 1st Floor, Madiwala, Hosur Road, Bangalore, PIN - 560 068 INDIA
Tel: +91 80 42033399 | Fax: +91 80 42033406 | URL: www.3i-corporation.com

Table of Contents

1 Introduction

1.1. Scope

This document is aimed in providing detailed information and complete listing as a reference to the Pegasus™ Studio - Configuration Tool.

1.2. Audience

This User Manual is intended for end users prepared to configure settings in the Pegasus™ Studio – Configuration Tool. Readers or end-users of this document should be familiar with Pegasus™ NX - Alarm Panel Communicator and the Zeus™ Server.

Note:

To get information about the Pegasus™ NX - Alarm Panel Communicator, refer the Pegasus™ NX – User Manual.

To get information about the Zeus™ Server, refer the Zeus™ Server – User Manual and the Zeus™ Server – Quick Start Manual.

1.3. Contact Information or Comments

For general contact, technical support, questions or comments to report documentation errors and suggestions, contact 3i-Corporation Technical Writing Team at: Basant.Mishra@3i-Corporation.com

Our aim is to make this user manual as helpful as possible. Keep us informed of your comments and suggestions for improvements. 3i-Corporation appreciates feedback from the users of our information.

1.4. Text Conventions

Begin Instruction:

To begin a procedure under any topic. Use a numbered list for points under procedure.

Note:

Provides a message or reminder related to a topic or section.

Warning:

Information provided under this section MUST be followed.

Caution:

To ensure proper unit operation, this product must be tested in accordance with 3i-Corporation standards. Reacceptance testing is required after any change, addition or deletion of unit components, or after any modification, repair or adjustment to unit hardware or wiring.

Important Information:

Provides important information related to a topic or section.

Tip:

Provides advice or suggestion related to a topic or section.

Troubleshooting:

Provides information to troubleshoot or fix any Pegasus™ NX related issues or problems.

2 Overview

2.1. About the User Manual

This User Manual describes how to configure settings related to Pegasus NX (device) by using the Pegasus™ Studio – Configuration Tool.The General Settings chapter step-by-step explains how to configure settings related to the general operations of the device. The GSM/GPRS chapter explains how to configure all the parameters related to the GSM/GPRS interface. The Ethernet chapter explains how to configure all the parameters related to the Ethernet interface. The Wi-Fi chapter explains how to configure all the parameters related to the Wi-Fi interface. The SMS chapter explains how to configure from which numbers Pegasus™ NX is allowed to receive messages. The Monitoring Station chapter explains how to configure settings related to the communication between Pegasus™ NX and the monitoring station using IP, GSM, CSD, SMS, etc.

The Write Configuration chapter explains how to write the configuration settings to device. The Write Configuration via SMS chapter explains how to write the configuration settings to divice via SMS. The Reboot Module chapter explains how to reboot your device after configuration.

The Save Configuration File chapter explains how to save the configuration file with Config file(*.bin) as the file type in your hard disk drive. The Open Configuration File explains how to open a previously saved configuration file with Config file(*.bin) extension from your hard disk drive. The Read Configuration chapter explains how to read the current configuration settings and save it to file for future use.

The Update Module Firmware chapter explains how to manually update Pegasus™ Modules firmware. The Events/Occurrences log chapter explains how to view and manage events/occurrences log. The Debug View chapter explains how to view and manage debug messages.

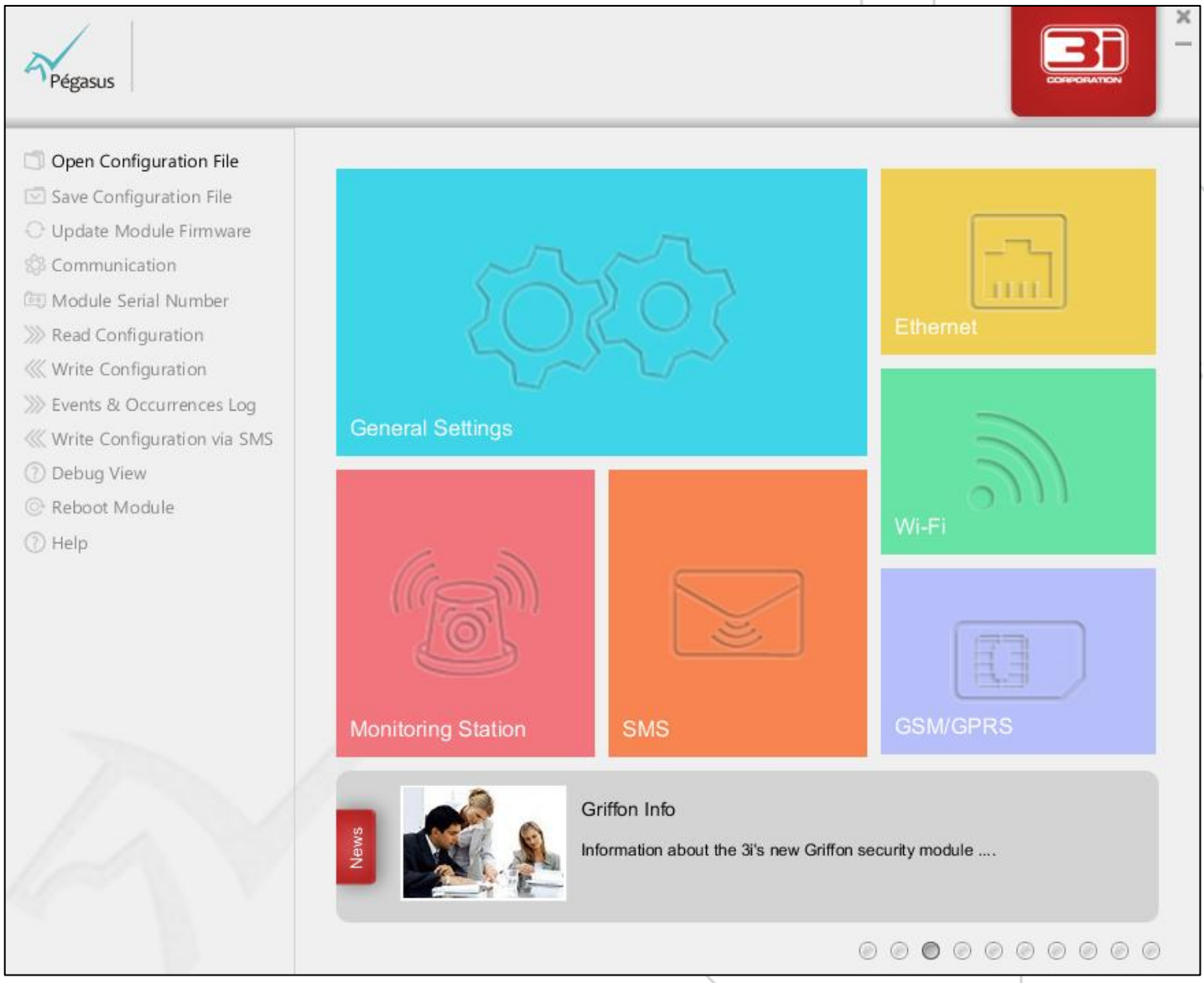
The Appendix chapter provides important information that might be needed while device configuration.

2.2. What is Pegasus™ Studio?

Pegasus™ Studio is a state-of-art installable application to assist you to accomplish your Pegasus™ Modules related configuration. Data configurability is one of the strengths of your Pegasus™ Module. You can configure various funtctions in its operation to adapt the device to different applications.

The Pegasus™ Studio Main Screen has six interfaces: General Settings, Ethernet, Wi-Fi, GSM/GPRS, SMS, and Monitoring Station.

This main screen is built-in 12 menu items: Open Configuration File, Save Configuration File, Update Module Firmware, Communication, Module Serial Number, Read Configuration, Write Configuration, Events & Occurrences Log, Write Configuration via SMS, Debug View, Reboot Module, and Help.



3 General Settings

The **General Settings** screen allows you to configure settings related to the general operations of Pegasus™ NX.

Configuration Instructions

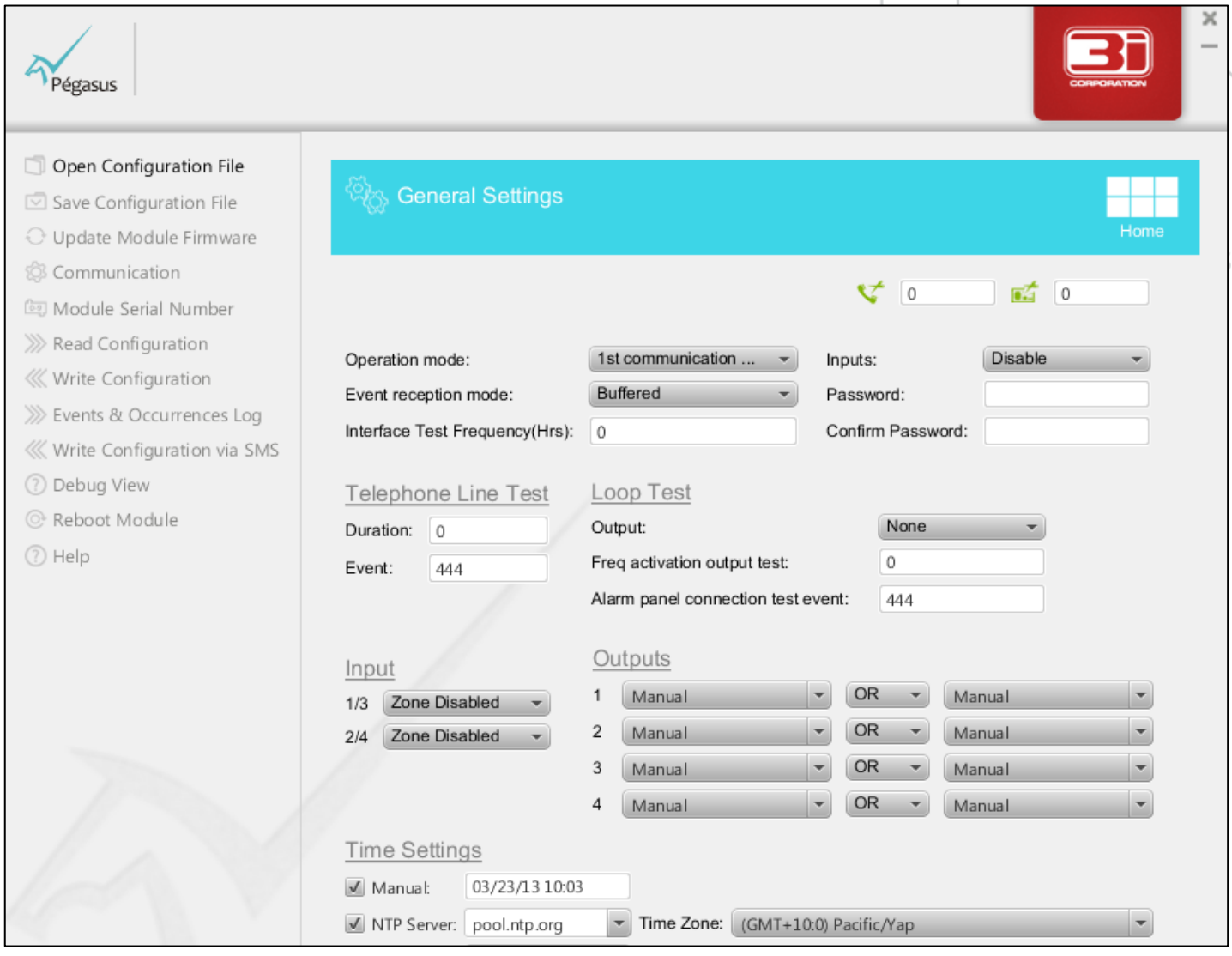
- To configure General Settings, follow steps: 3.1 to 3.14.
- To configure additional delay duration in telephone line cut off detection, follow steps: 3.3. Enable Telephone Line Cut Off Detection, and 4.4. Configure Additional Delay Duration in Telephone Line Cut OFF Detection.
- To configure additional delay duration in alarm panel return cut off detedtion, follow steps: 3.5. Enable Alarm Panel Return Cut Off Detection, and 3.6. Configure Additional Delay Duration in Alarm Panel Return Cut Off Detection.
- To write the General Settings configuration to Pegasus NX, follow step 3.12. Write Configuration. To apply the General Settings configuration, follow step 3.13. Reboot Module.

3.1. Open the General Settings Screen

To open the general settings screen

1. On the **Pegasus™ Studio Main Screen**, place your cursor on the **General Settings** section, and then click to open the **General Settings** screen.

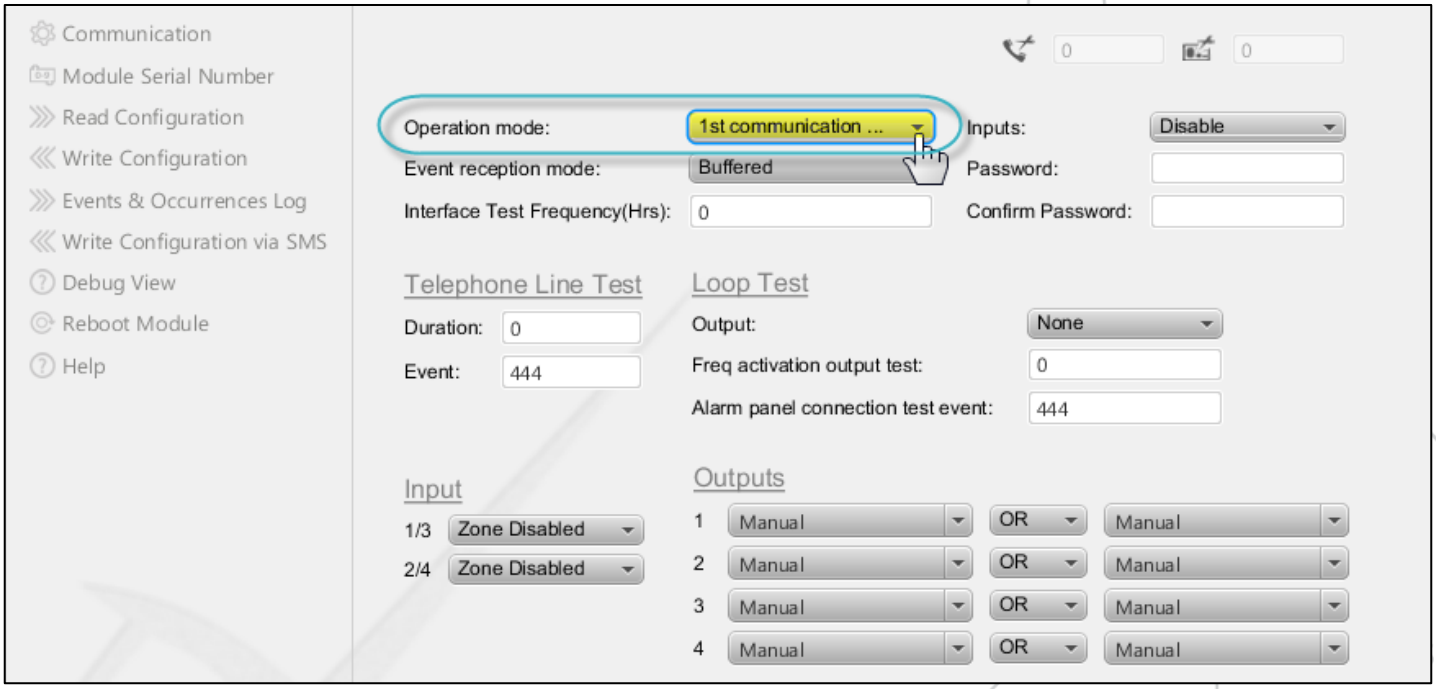
The **General Settings** screen is displayed as shown below.



3.2. Configure General Settings

To configure general settings

1. In the **Operation Mode** drop-down box, select **1st Communication Path** or **2nd Communication Path**.



Important Information: First Communication Path & Second Communication Path

First Communication Path

The first communication path includes: GPRS, Wi-Fi and Ethernet. Pegasus™ NX sends event(s) received from the alarm panel to the Zeus™ Server via first communication path (if first communication path is selected as the operation mode). In the first communication path, telephone acts as a backup.

In the first communication path, Pegasus™ NX preferably attempts to transmit events through GPRS, Wi-Fi and Ethernet. In case of failure like GPRS, Wi-Fi and Ethernet down, Zeus™ Server unavailable or connection timeout with many retries, it switches to second communication path which gives the telephone line back to the alarm panel. If any cut off is found in the telephone line, then Pegasus™ NX waits for 30 seconds in addition to the configured delay time, if the telephone line is not restored within this time, then the events are transmitted through CSD data call or SMS or GSM voice call using DTMF for sending events, and tone detection by opamp circuits for receiving ACK.

Second Communication Path

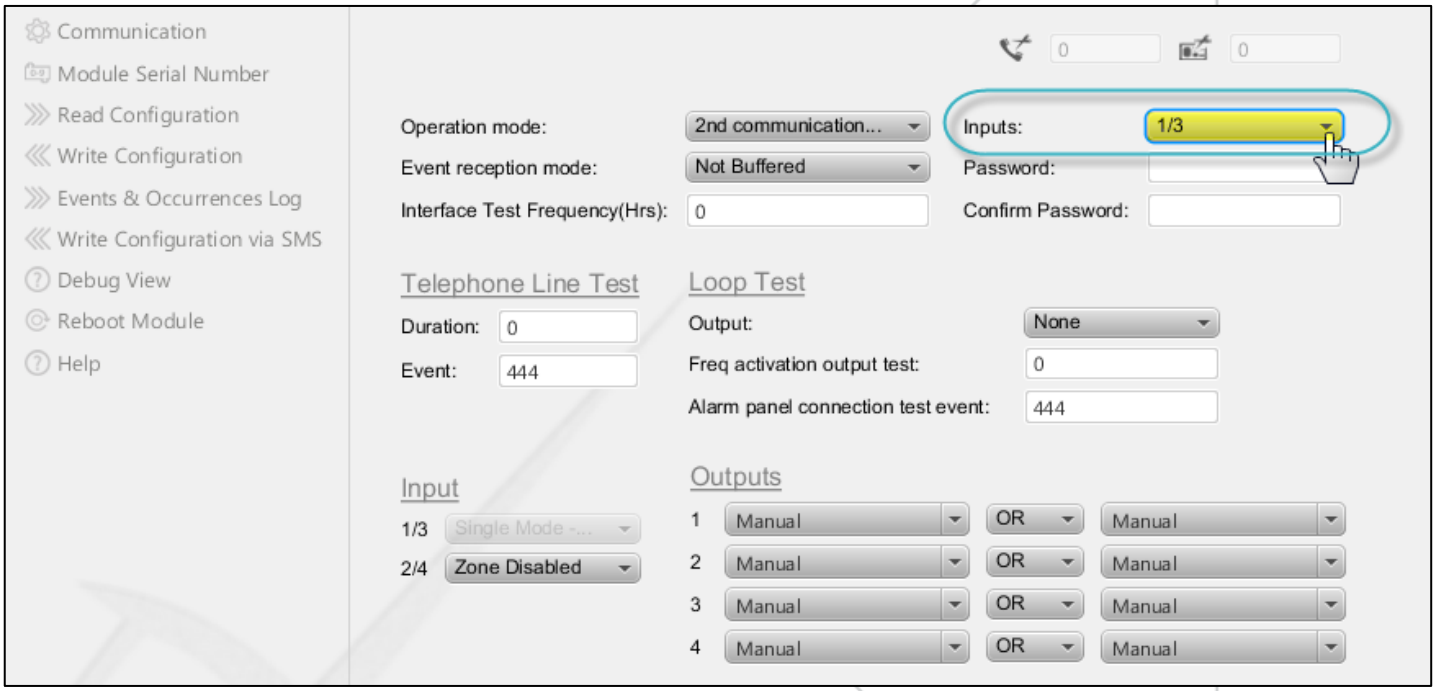
The second communication path is telephone. Pegasus™ NX sends event(s) received from the alarm panel to the Zeus™ Server via second communication path (if the second communication path is selected as the operation mode).

In second communication path, Pegasus™ NX first gives the telephone line to the alarm panel. If any failure (line cut off) is there, then the events are transmitted through GPRS, WiFi or Ethernet. Here, the first communication path is telephone, and the second communication path is GPRS, Wi-Fi and/or Ethernet. In the second communication path, the first communication path acts as a backup.

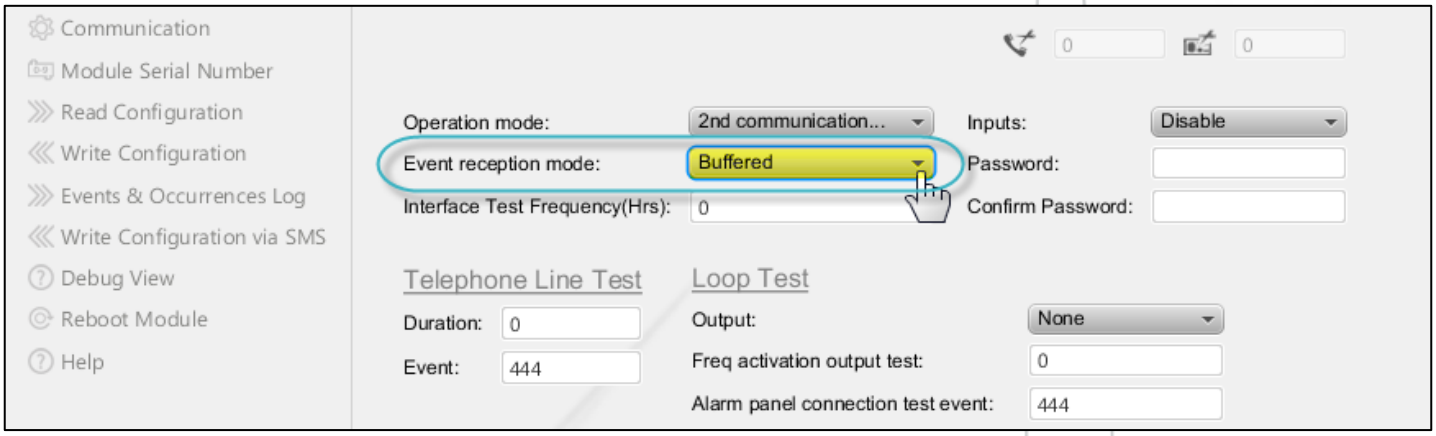
Note:

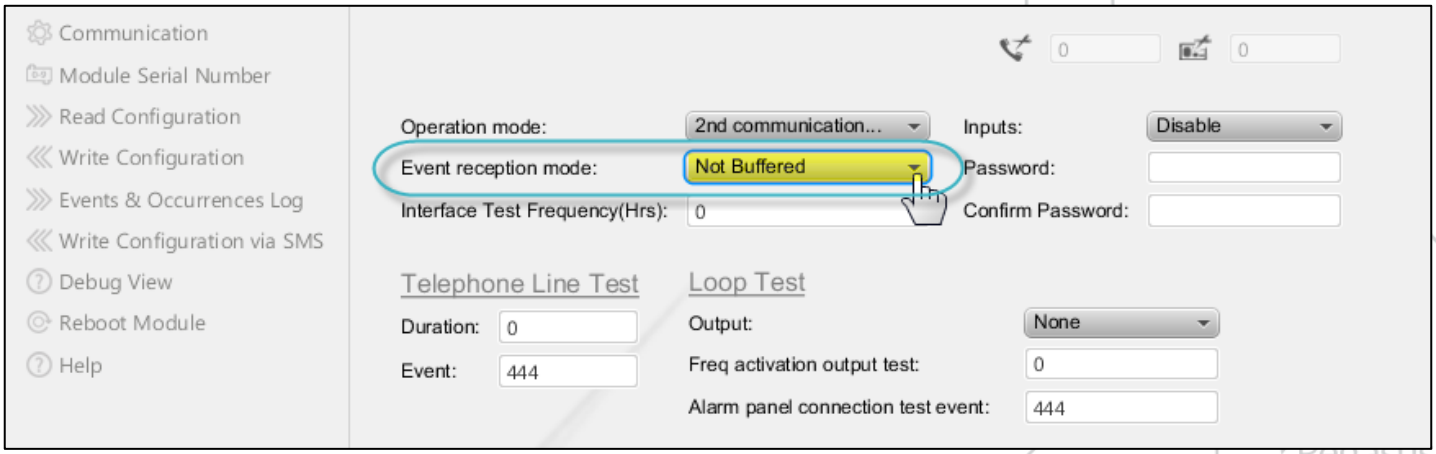
- In Pegasus™ Full Module, GPRS, Wi-Fi, and Ethernet are available as the first communication path.
- In Pegaus™ (GPRS + Ethernet) Module, both GPRS and Ethernet are available as the first communication path.
- In Pegasus™ Wi-Fi Module, only Wi-Fi is available as the first communication path.
- In Pegaus™ GPRS Module, only GPRS is available as first communication path.

2. In the **Inputs** drop-down box, select an input for control operation mode. You can select input **1/3** or **2/4.** To restrict the input mode, in the **Inputs** drop-down box, select the **Disable** option.



3. In the **Event Reception Mode** drop-down box, select the **Buffered** or **Not Buffered** option.





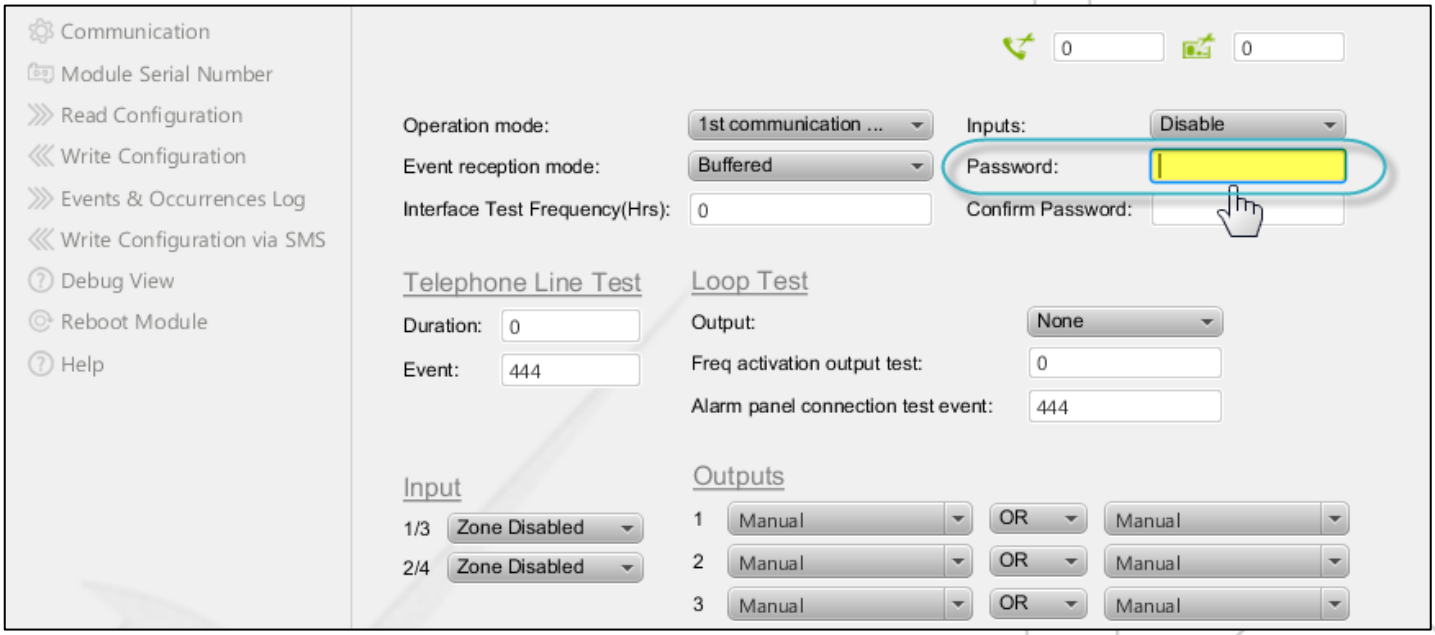
Important Information:

The Event Reception drop-down box offers two event reception modes: Buffered and Not Buffered.

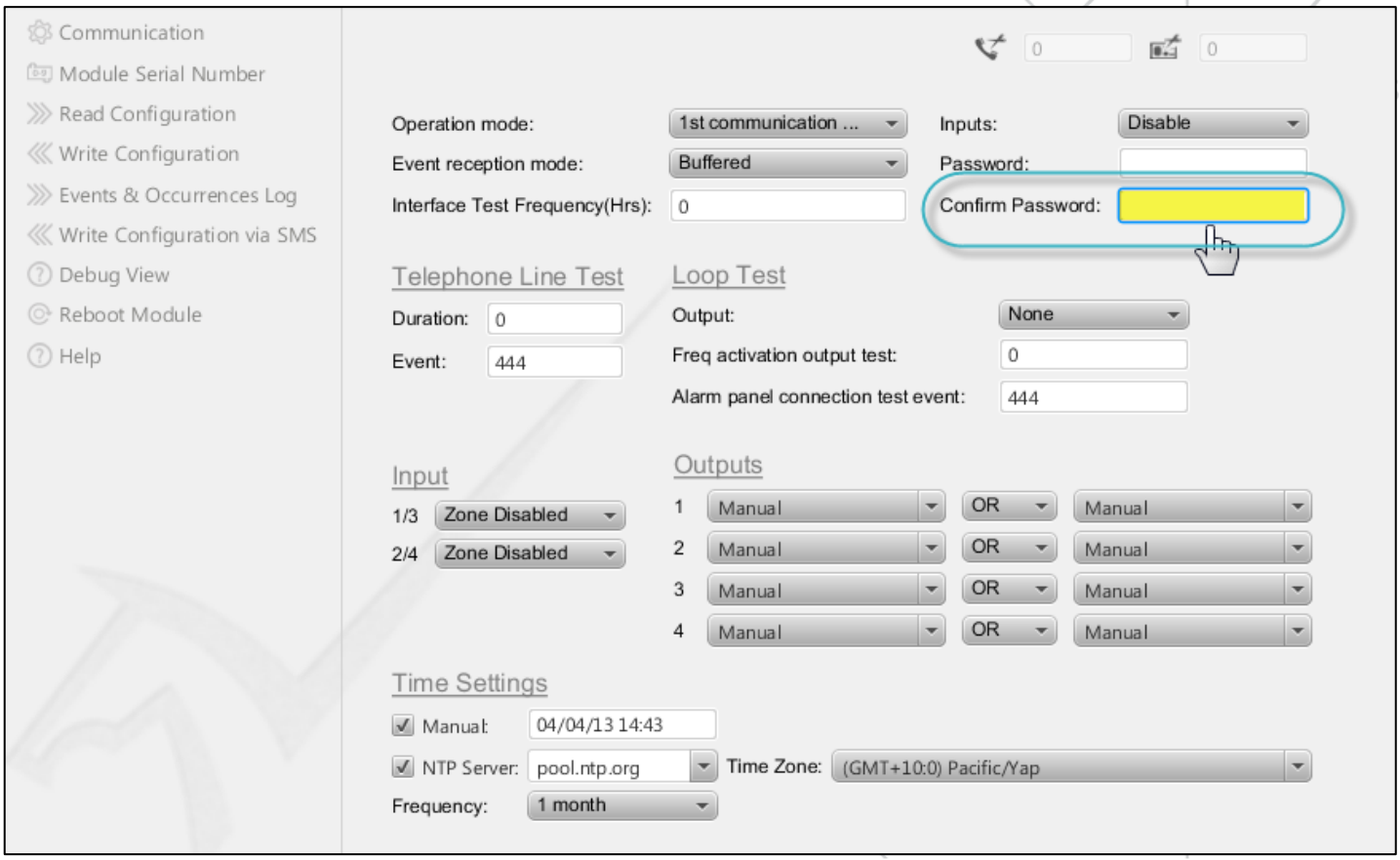
In the Buffered Mode, Pegasus™ Studio uses a flash memory storage to temporarily hold events while it is being moved to the Zeus™ Server. Pegasus™ NX receives event and checks the communication status with the Zeus™ Server, saves the event in its memory and generates the Kiss-off tones to the alarm panel, and then the event is sent to the Zeus™ Server. Use the Buffered Mode if you want Pegasus™ NX to buffer events before sending it to the Zeus™ Server.

In Not Buffered Mode, any event received by Pegasus™ NX from the alarm panel is not buffered. Once an event is received, Pegasus™ NX sends it directly to the Zeus™ Server without buffering. On successful event reception, the Zeus™ Server sends an acknowledgement to Pegasus™ NX, which in turn sends an acknowledgement to the alarm panel. In this reception mode, Kiss-off tones are generated to the alarm panel only after confirmation from the Zeus™ Server that the event was successfully stored in its database. Use the not buffered option if you want Pegasus™ NX to send occurrences to the Zeus™ Server without buffering.

4. In the **Password** text box, enter your **password**.



5. To confirm your password, in the **Confirm Password** text box, type-in the same password you entered in the **Password** text box.



Note:

The Password text box can be used to set password for programming. Password is required to authenticate your credentials to modify the Pegasus™ Studio configuration settings.

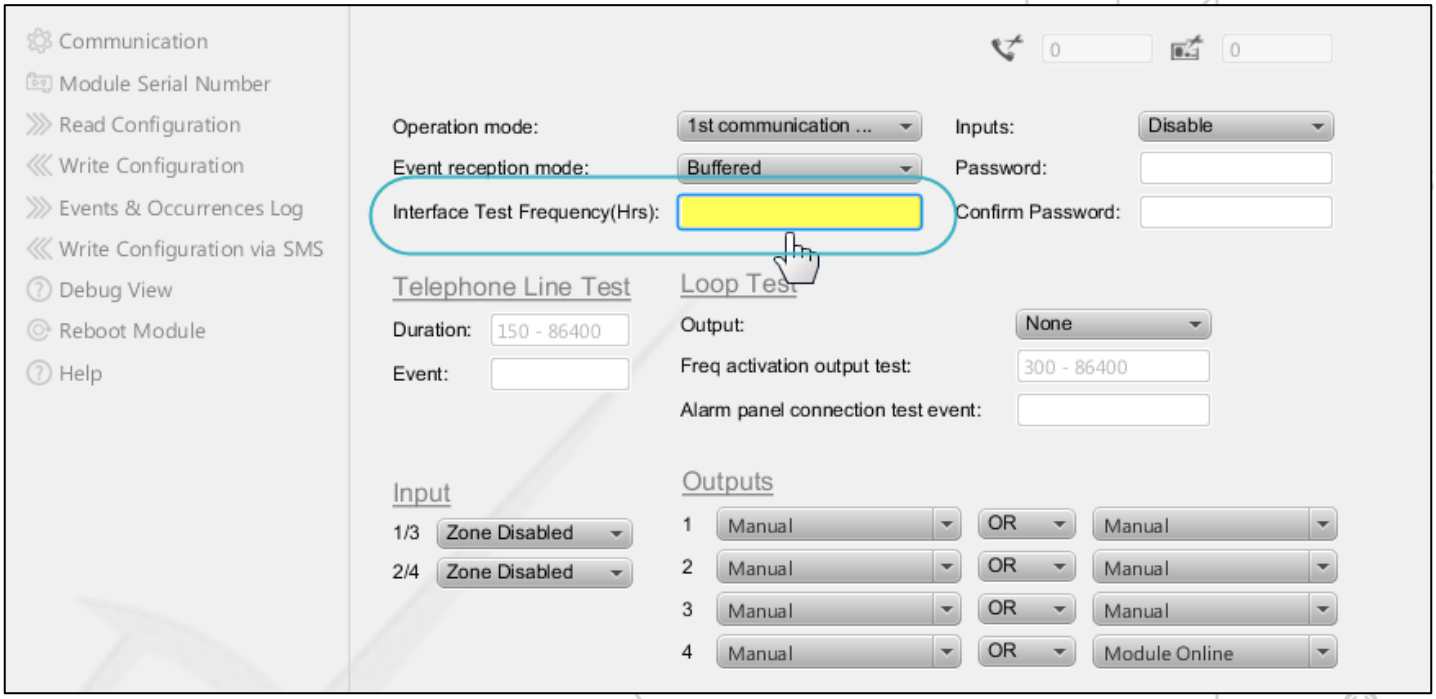
You can enter upto nine character password. Password beyond nine character is not allowed. You can use alphabets, special characters and numbers to make your password more secure.

Caution:

Your password should be confidential. Never disclose your Pegasus™ Studio password to any individual. Change your password regularly.

6. In the **Interface Test Frequency (Hrs)** text box, type-in the interface test frequency duration in hours.

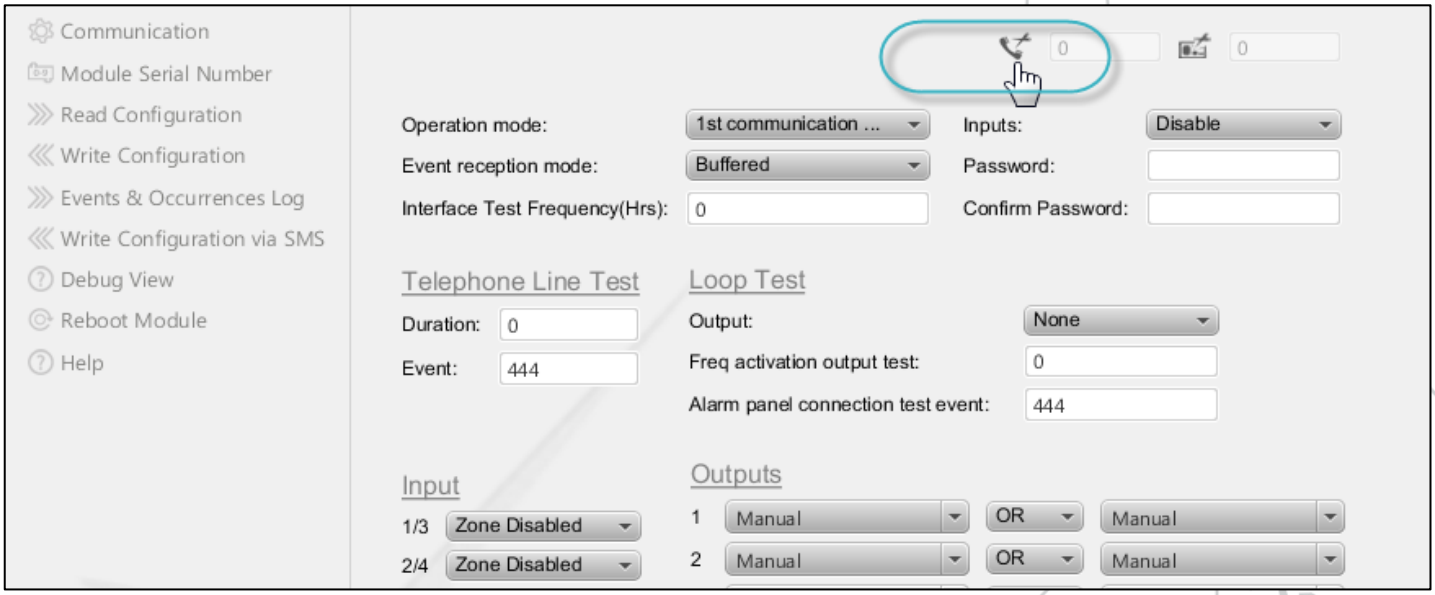
   The minimum acceptable duration is six hours and the maximum duration is 240 hours.



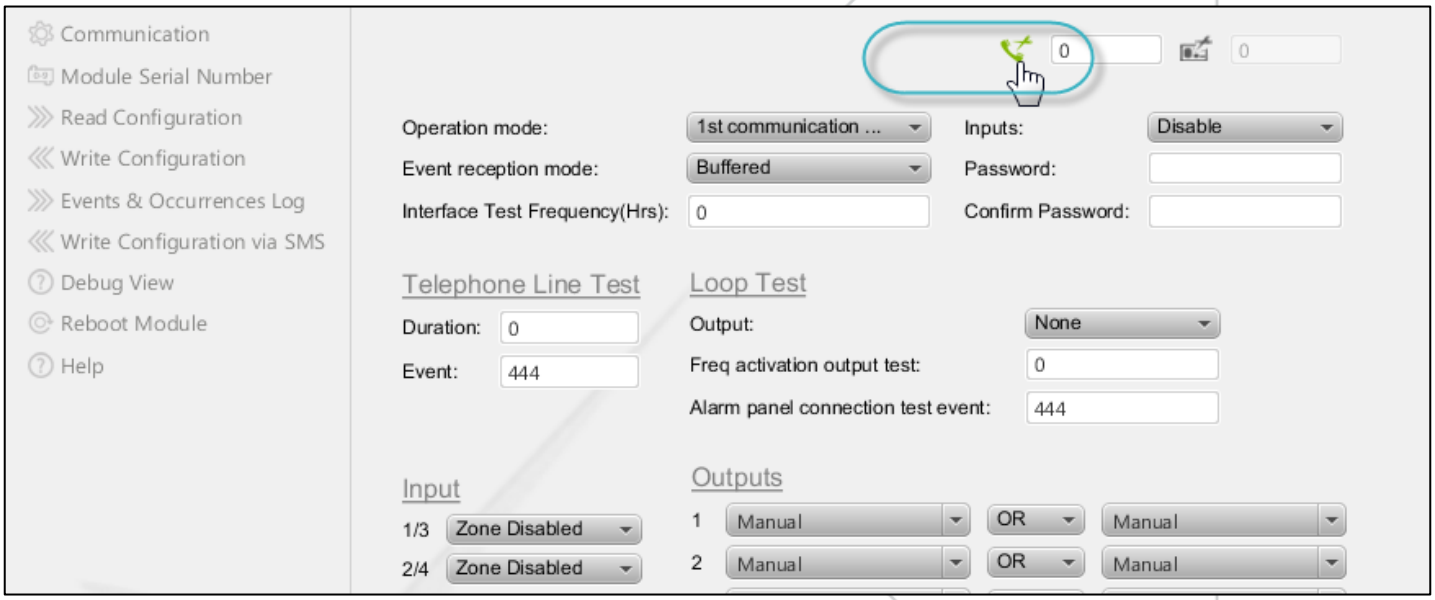
3.3. Enable Telephone Line Cut Off Detection

To enable telephone line cut off detection

1. Click the grey colored **Detect Telephone Line Cut Off**  icon.



2. The grey colored icon is turned green  as shown in the below image. The **Detect Telephone Line Cut Off** feature is in the enabled state.

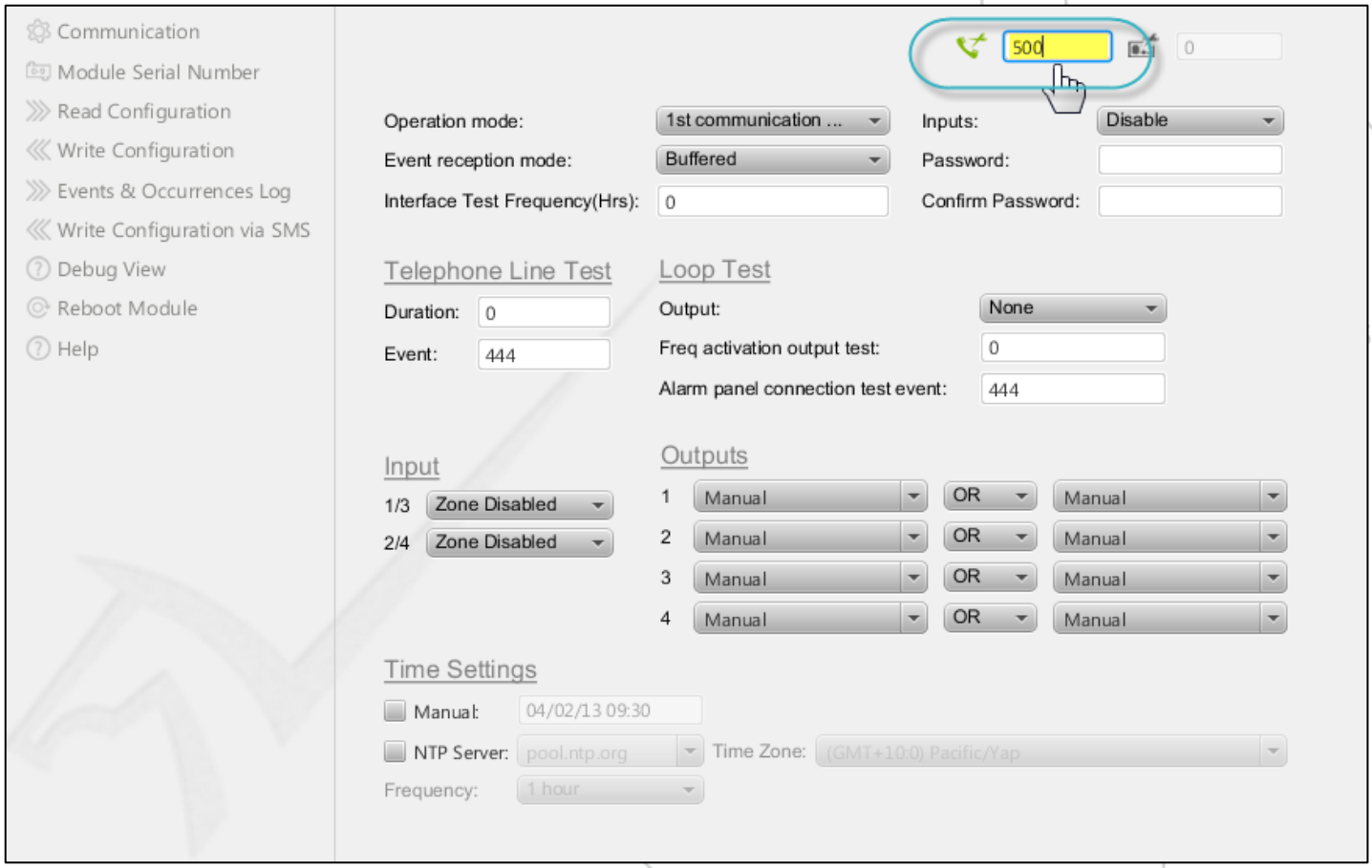


3.4. Configure Additional Delay Duration in Telephone Line Cut OFF Detection

Telephone Line Cut Off Detection allows you to detect telephone line cut off and thus makes the security system more consistent. If telephone line cut off detection is enabled, by default, detection of telephone line cut off occurs after every 30 seconds. You can also configure the additional delay duration in telephone line cut off detection.

To configure additional delay duration in telephone line cut off detection

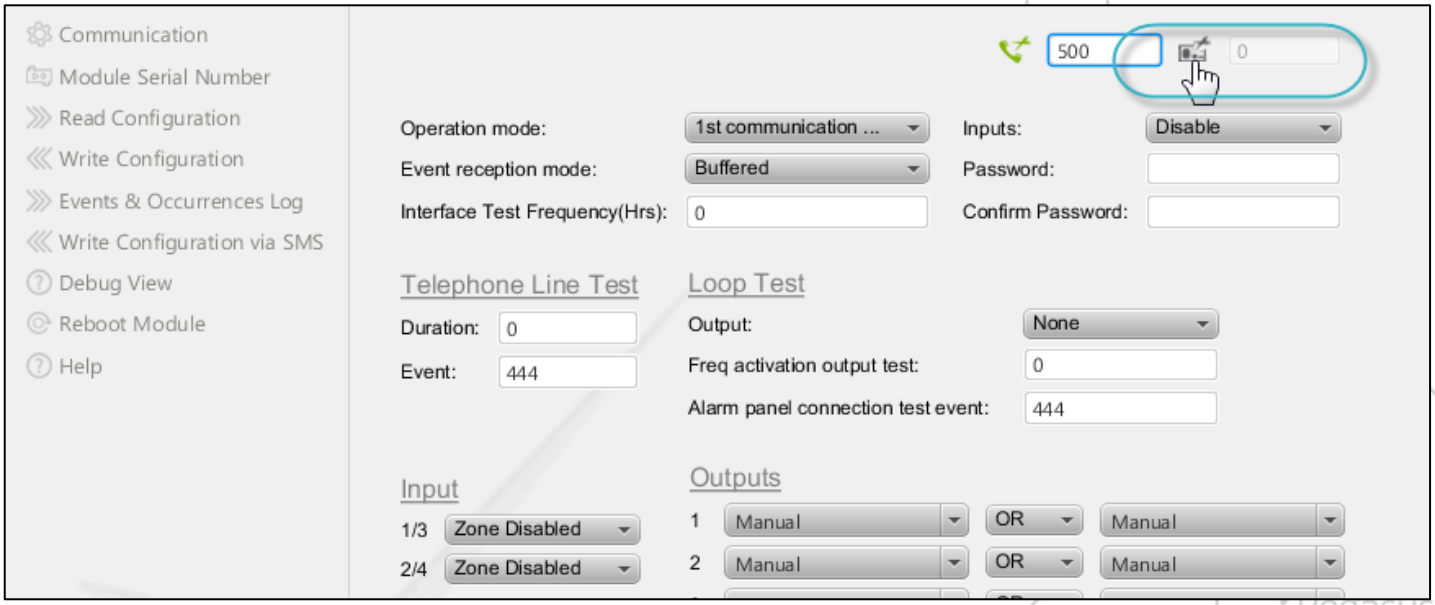
1. In the **Telephone Line Cut OFF Detection** text box, enter the additional delay duration in telephone line cut off detection in seconds (minimum duration – 0 second, maximum duration – 86400 seconds and default duration – 0 second).



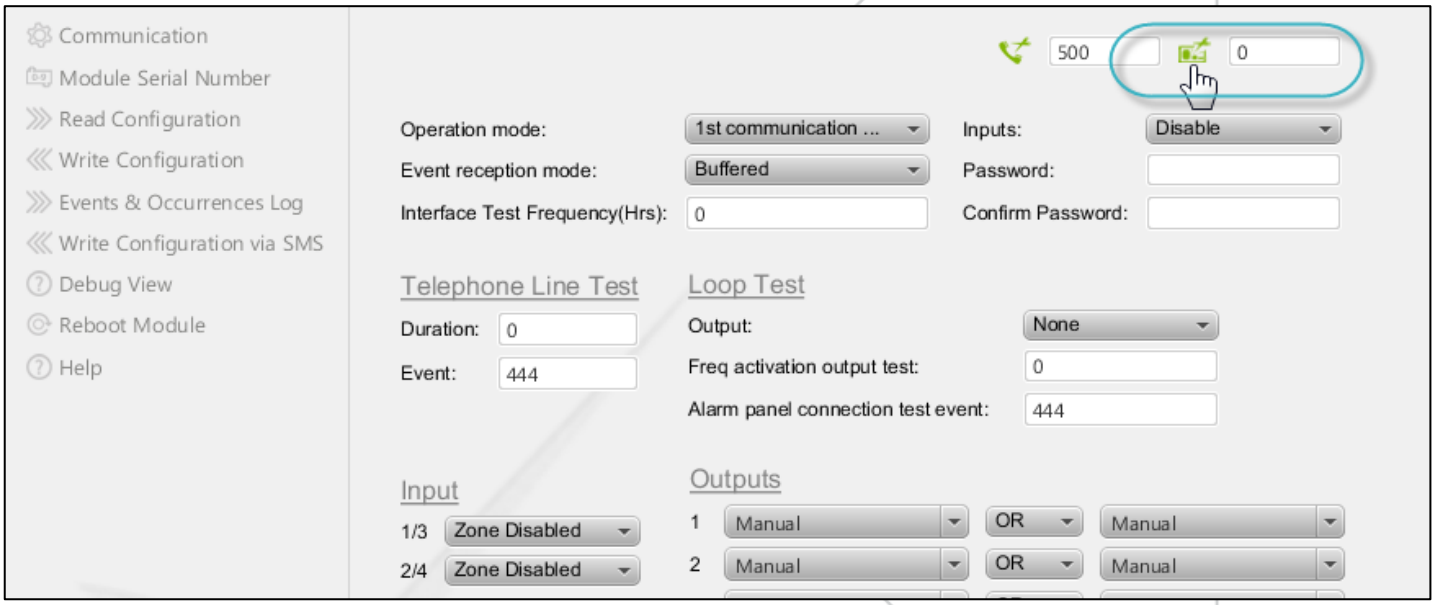
3.5. Enable Alarm Panel Return Cut Off Detection

To enable alarm panel return cut off detection

1. Click the grey colored **Detect Alarm Panel Return Cut Off**  icon.



2. The grey colored icon is turned green  as shown in the below image. The **Detect Alarm Panel Return Cut Off** feature is in the enabled state.

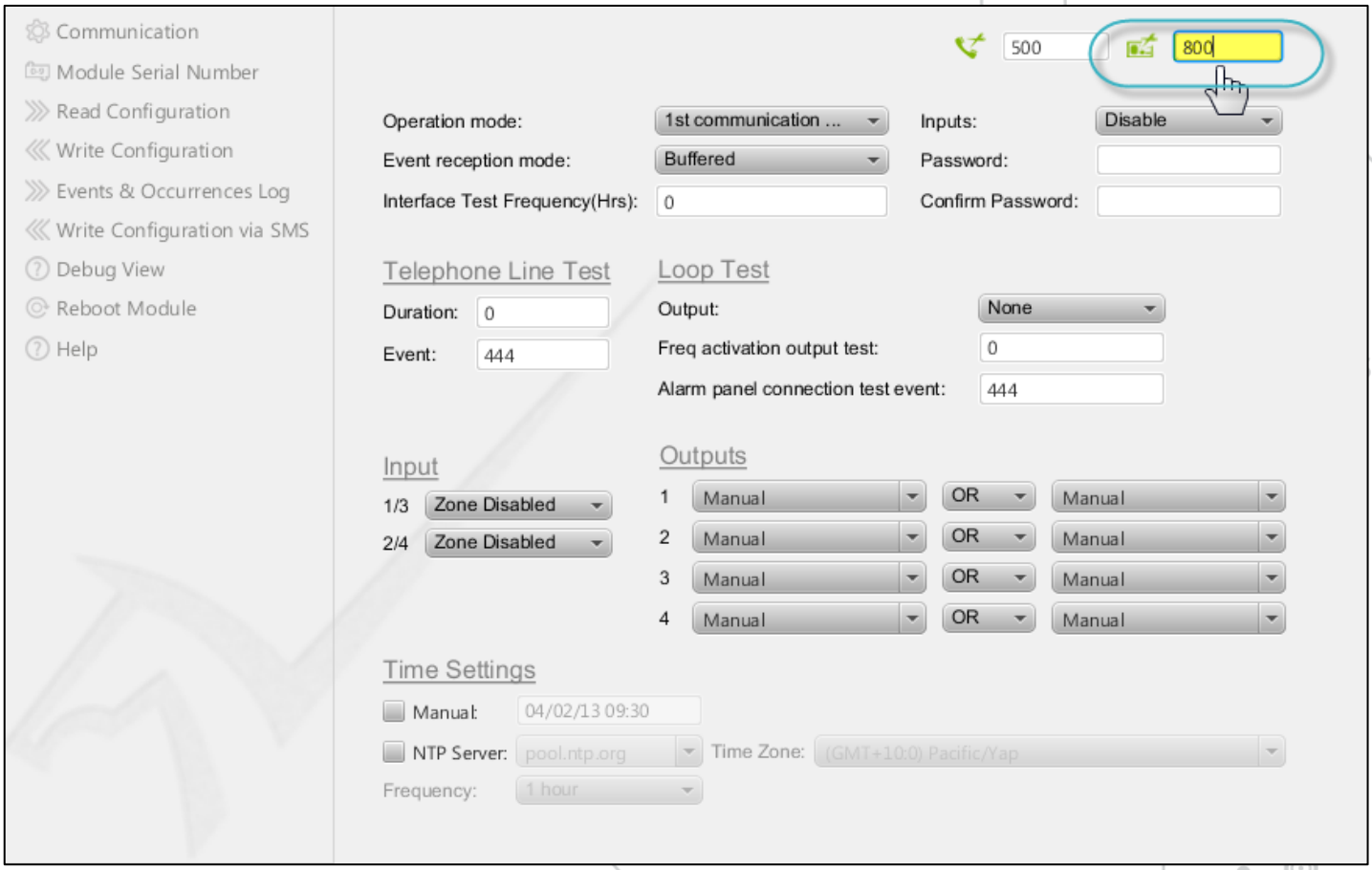


3.6. Configure Additional Delay Duration in Alarm Panel Return Cut Off Detection

Alarm Panel Return Cut OFF Detection allows you to detect alarm panel return cut off, and thus makes the security system more consistent. You can also configure additional delay duration in the alarm panel return cut off detection.

To configure additional delay duration in the alarm panel return cut off detection

1. In the **Alarm Panel Return Cut OFF Detection** text box, enter the additional delay duration in the alarm panel return cut off detection in seconds (minimum duration – 0 second, maximum duration – 86400 seconds & default duration – 0 second).



3.7. Configure Telephone Line Test

Telephone Line Test is generally done to verify the working status of the telephone line which is made available to the alarm panel for a fixed duration, a predefined test event code is set, configuration is written to Pegasus™ NX, and then module is rebooted.

In Debug View, a 16 digit message composition as per the contact id protocol is shown along with the predefined test event code. Match and verify the test event code with the event code received in the message composition. The event will not be transmitted to the monitoring station as it is a predefined telephone line test event.

Additional Information: Message Composition** as per Contact ID Protocol

The form of the message is: ACCT MT QXYZ GG CCC, where: ACCT = 4 Digit Account Number (0-9, B-F)

MT = MESSAGE TYPE
This two digit sequence is used to identify the Contact ID message to the receiver. It may be transmitted as either 18 (preferred) or 98 (optional). New receiver implementations shall accept either a 18 or a 98. Note that some older receivers may not accept 98 .

Q = EVENT QUALIFIER
Gives specific event information: 1 = New Event or Opening, 3 = New Restore or Closing, and 6 = Previously reported condition still present (Status report).

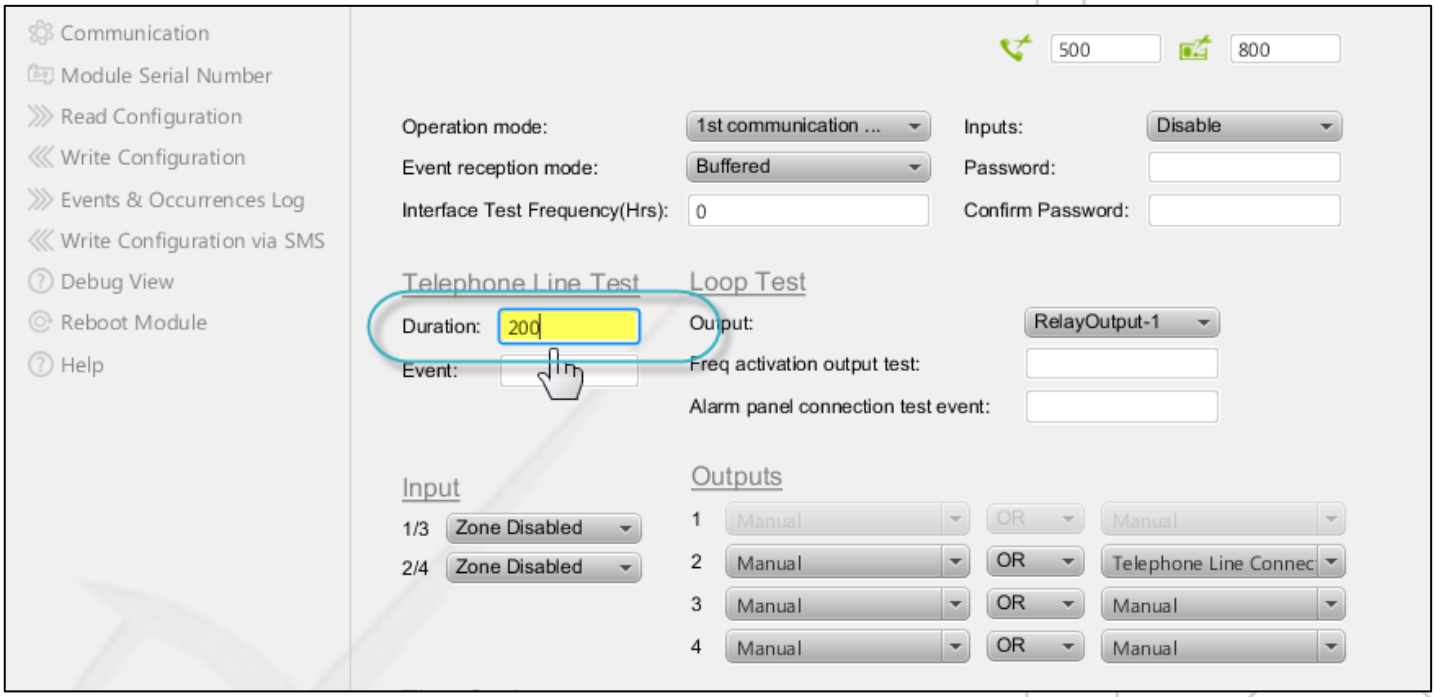
XYZ = EVENT CODE: 3 Hex digits 0-9, B-F

GG = GROUP OR PARTITION NUMBER
Two Hex digits 0-9, B-F. Use 00 to indicate that no specific group or partition information applies.

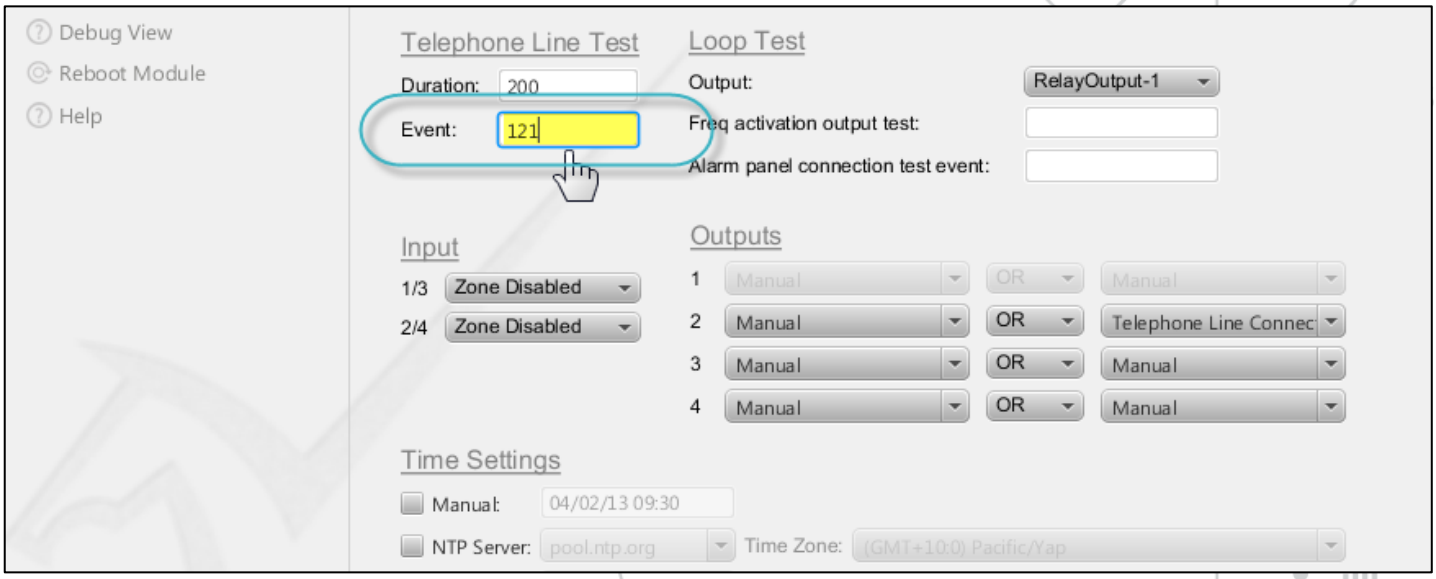
CCC = ZONE NUMBER
Event reports or User #: Open/Close reports, 3 Hex digits 0-9, B-F. Use 000 to indicate that no specific zone or user information applies S = 1 Digit Hex checksum calculated such that: (Sum of all message digits + S) MOD 15 = 0

To configure telephone line test

1. In the **Duration** text box, enter the total duration during which the telephone line is made available to the alarm panel in seconds. The minimum acceptable duration is 150 seconds and the maximum acceptable duration is 86400 seconds. The default duration is 150 seconds.



2. In the **Event** text box, enter the predefined **test event code**. The acceptable value of test event can be of 3/5/8 digits. The event code allows: digits 0-9 and alphabets B-F.



3. To apply the telephone line test configuration settings and make it functional, write configuration to Pegasus™ NX, and then reboot module.

4. In the **Debug View** screen, a message composition** as per the contact id protocol is shown. Verify and match the event code* (XYZ) in the message composition** with the test event code.

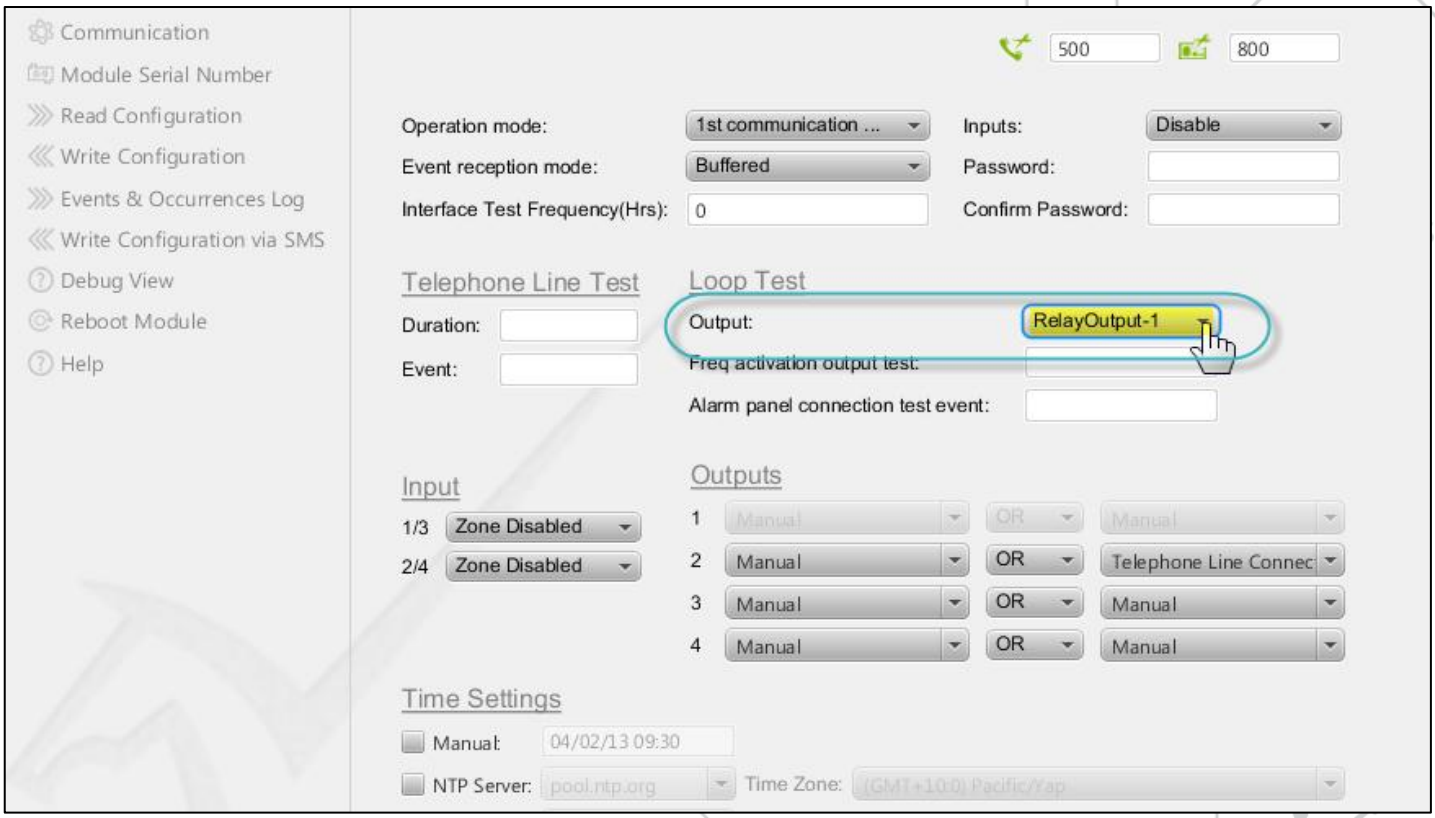
3.8. Configure Loop Test

Loop Test is generally done to verify the working status of the alarm panel connection. Here, a relay output is selected, frequency (number of occurrences of a repeating event per unit time) of the loop test and a predefined alarm panel connection test event code is set, configuration is written to Pegasus™ NX, and then module is rebooted. In Debug View, a 16 digit message composition as per the contact id protocol is shown along with the predefined alarm panel test event code. Match and verify the alarm panel test event code with the event code received in the message composition. This event will not be transmitted to the monitoring station as it is a test event used to check the alarm panel connection.

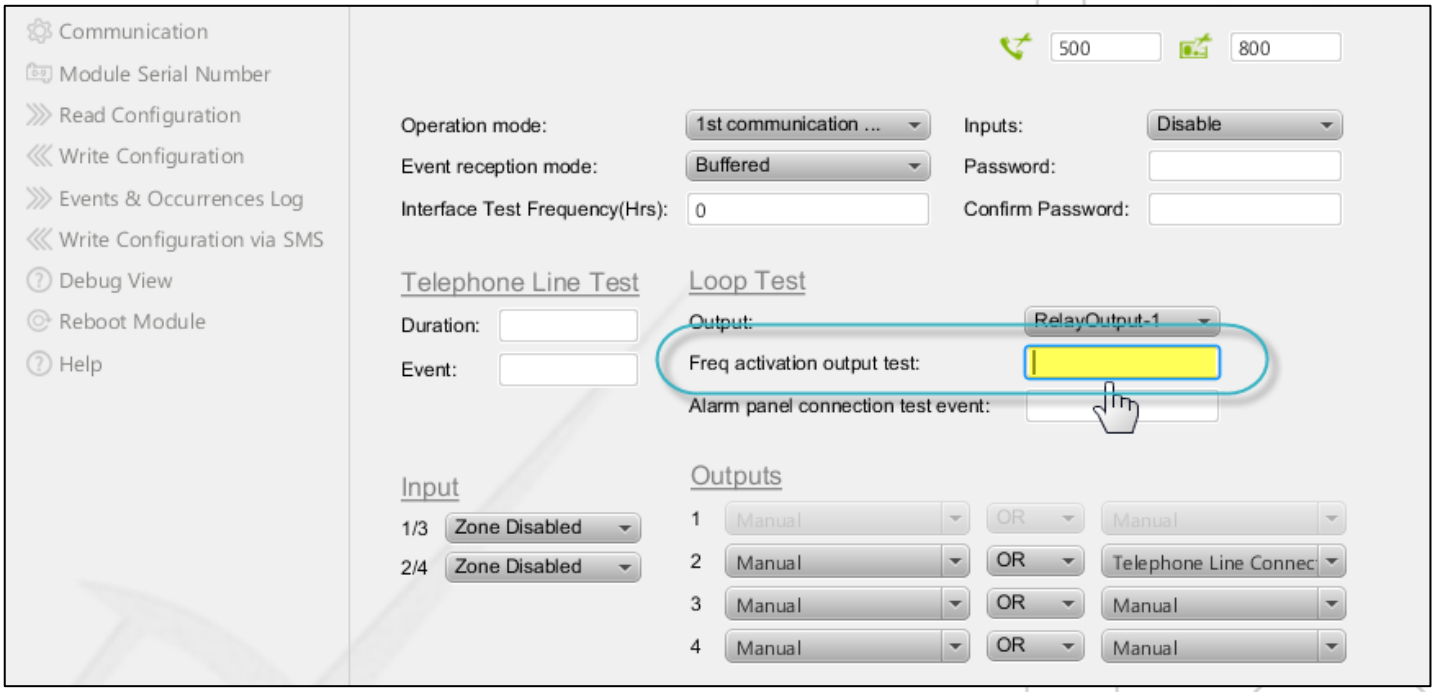
In case Pegasus™ NX fails to receive any test event from the alarm panel, it will try the alarm panel loop test two more times, if again failed to receive any test event, then an occurrence related to the alarm panel connection failure is sent to the Zeus™ Server.

To configure the alarm panel loop test

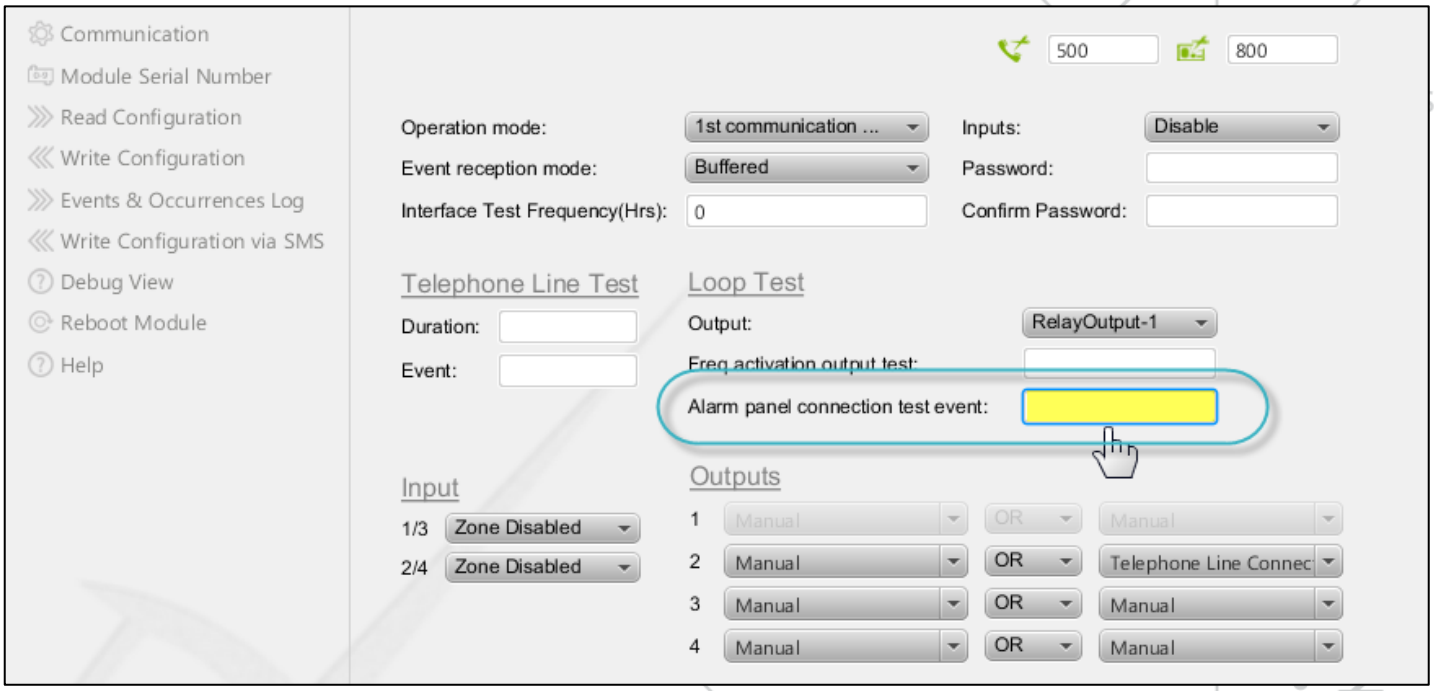
1. In the **Output** drop-down box, select a relay output for the loop test. Four relay outputs are available.



2. In the the **Freq Activation Output Test** text box, enter the number of occurrences of the loop test in seconds. The minimum acceptable duration is 300 seconds and the maximum acceptable duration is 86400 seconds. The default duration is 0.



3. In the **Alarm Panel Connection Test Event** text box, enter your predefined test event codeas per the contact id protocol.



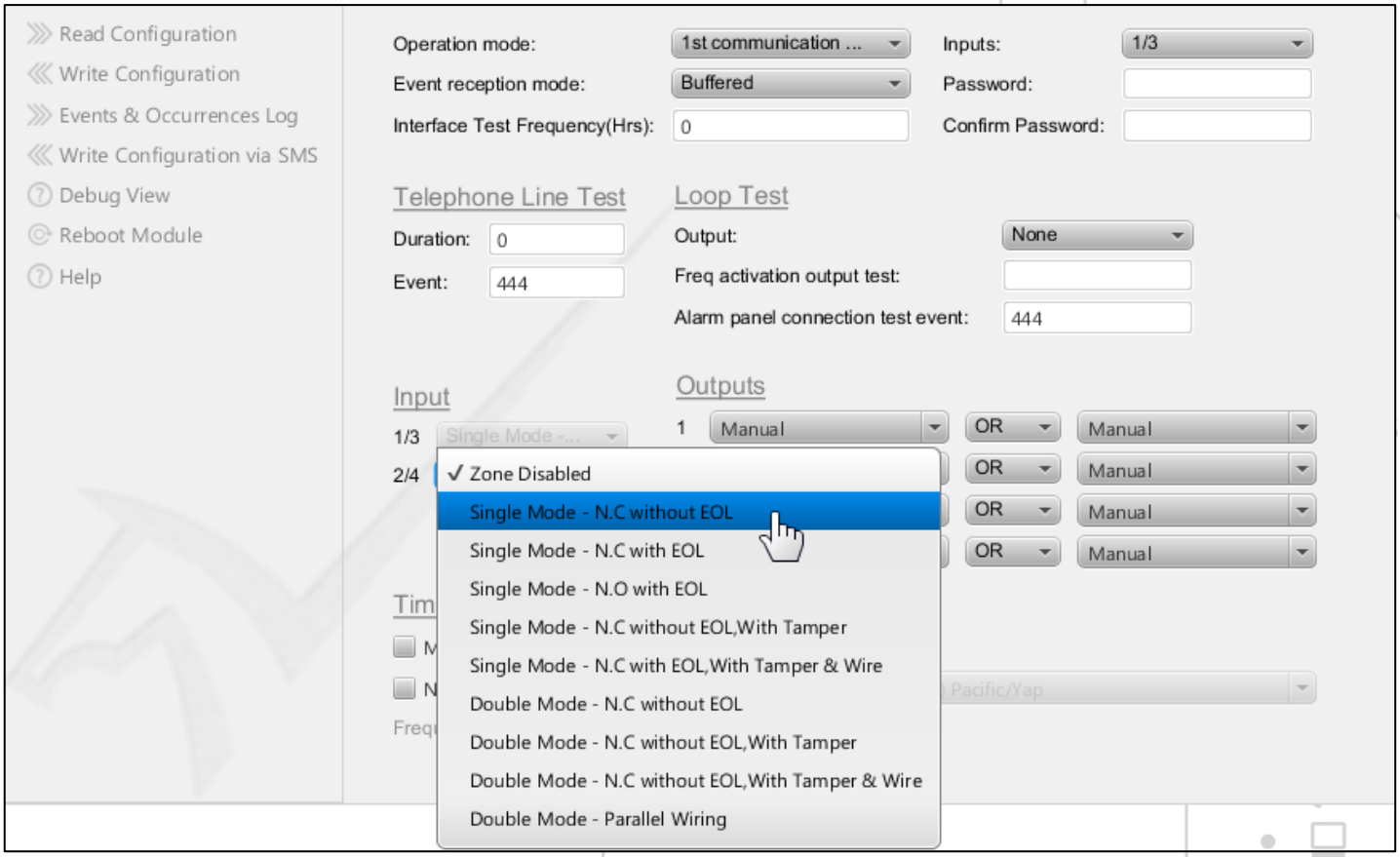
3.9. Configure Zone Inputs

Pegasus™ NX is built-in two zones which are extended to four zone inputs as shown in image. You can connect sensors or detectors to these zones.

Pegasus NX supports zone input wiring in both single-mode and double-mode. A sensor or detector can be connected in nine different ways.

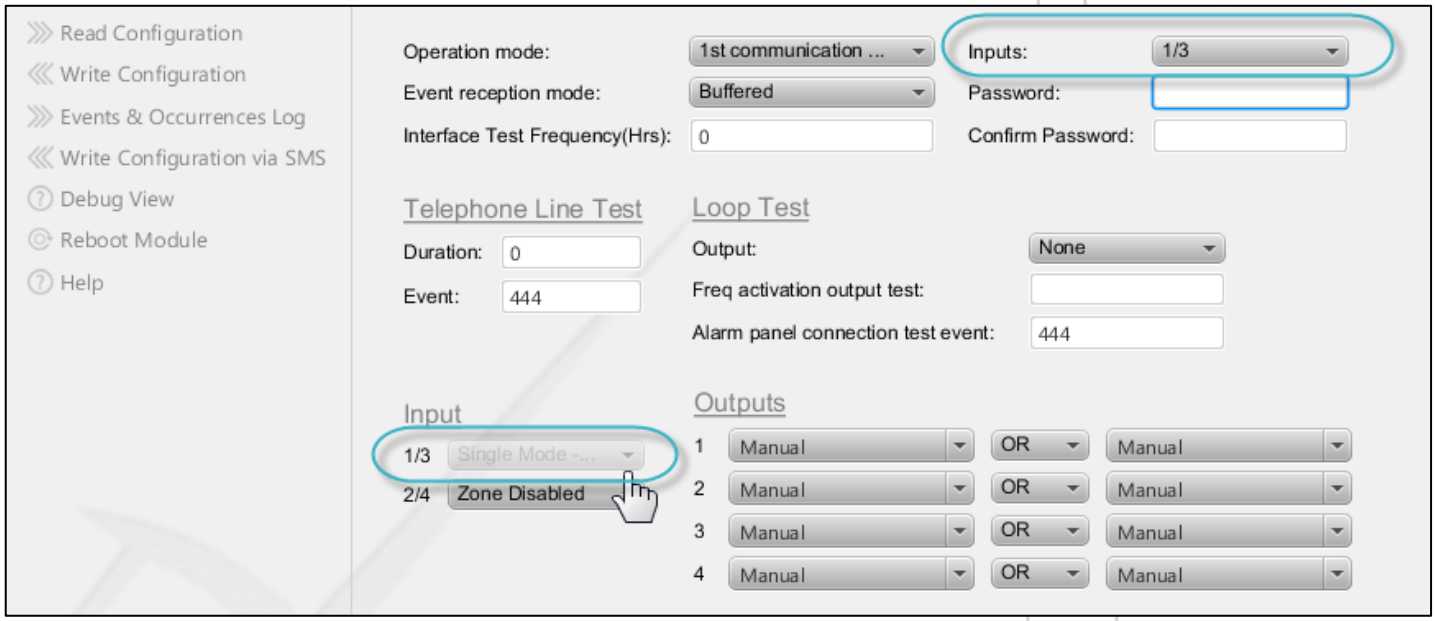
To configure zone input

1. In **Zone 2/4** drop-down box, select an **Input for Zone 2/4**.



Note:

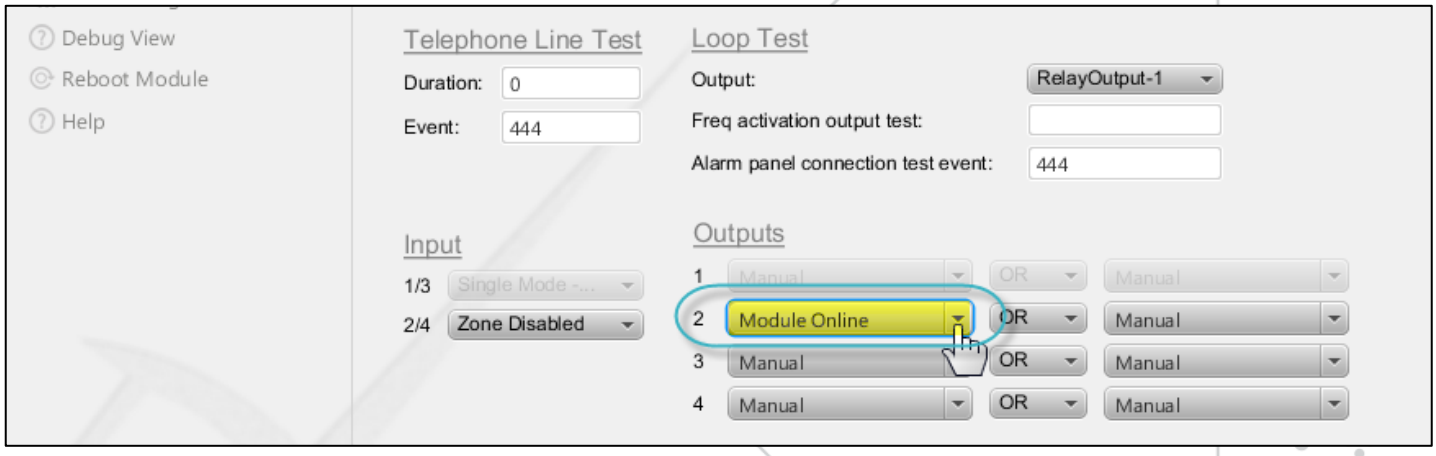
Here. **Input 1/3** drop-down box is in disabled mode as **Input 1/3** is already selected as the **Input for Operation Mode.**



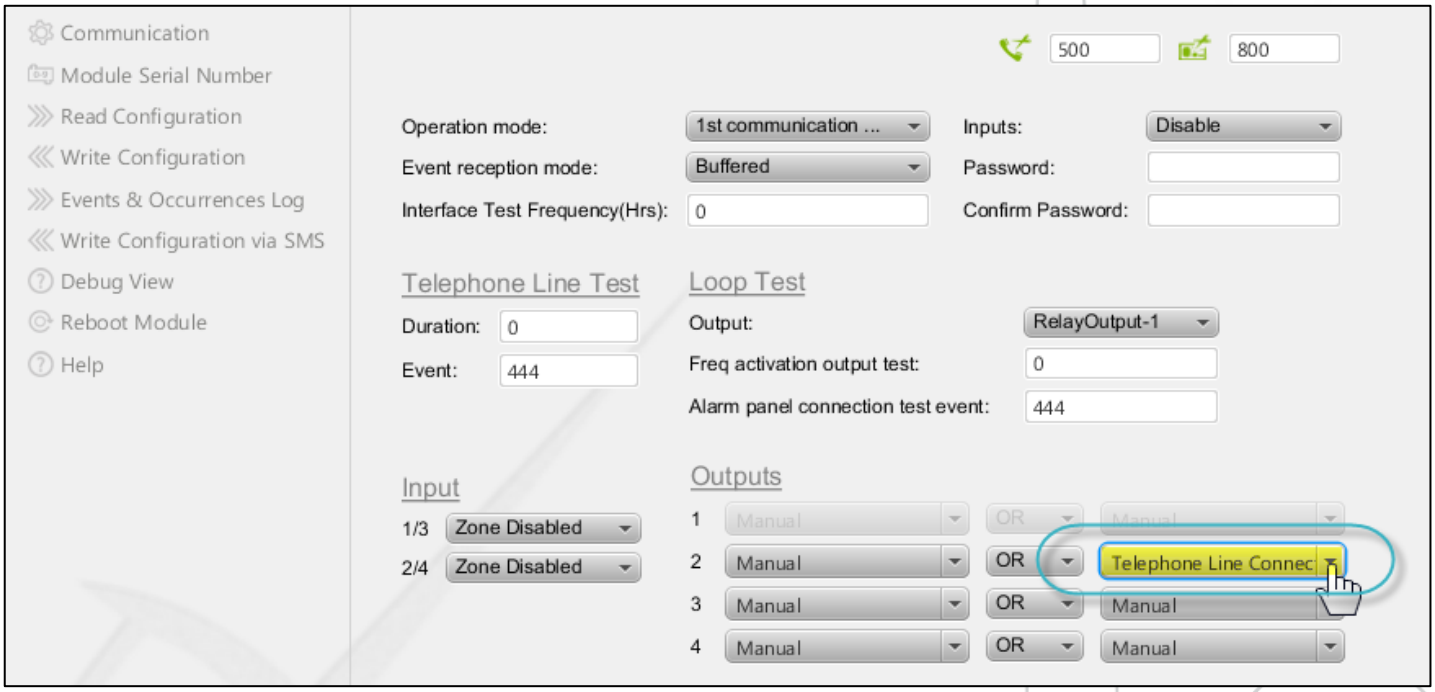
3.10. Configure Relay Outputs

To configure relay outputs

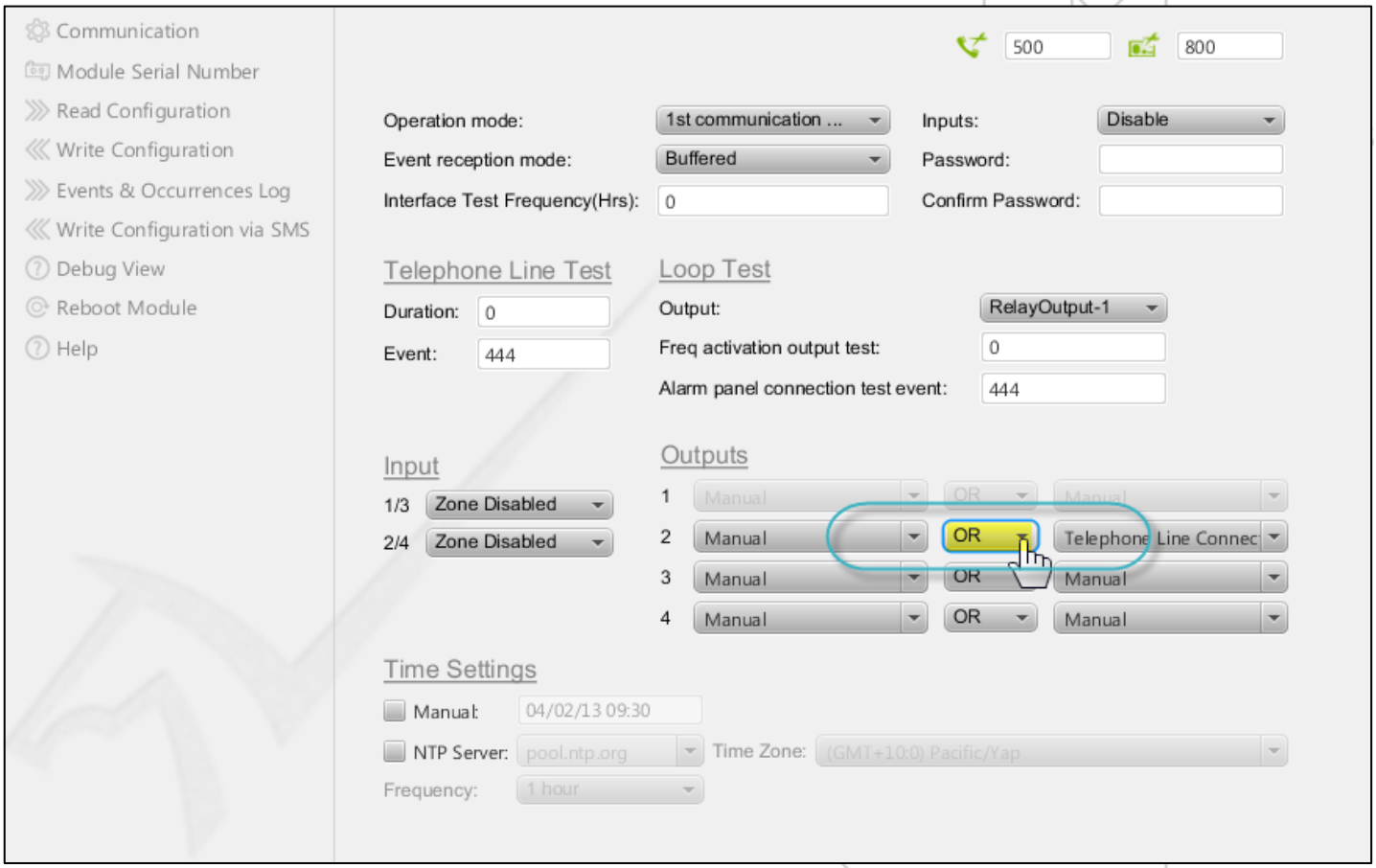
1. Under Outputs 2, select an output option from the first drop-down box as shown in the below image. Total 42 output options are available for selection.



2. Under Outputs 2, select an output option from the third drop-down box as shown in the below image. Total 42 output options are available for selection.

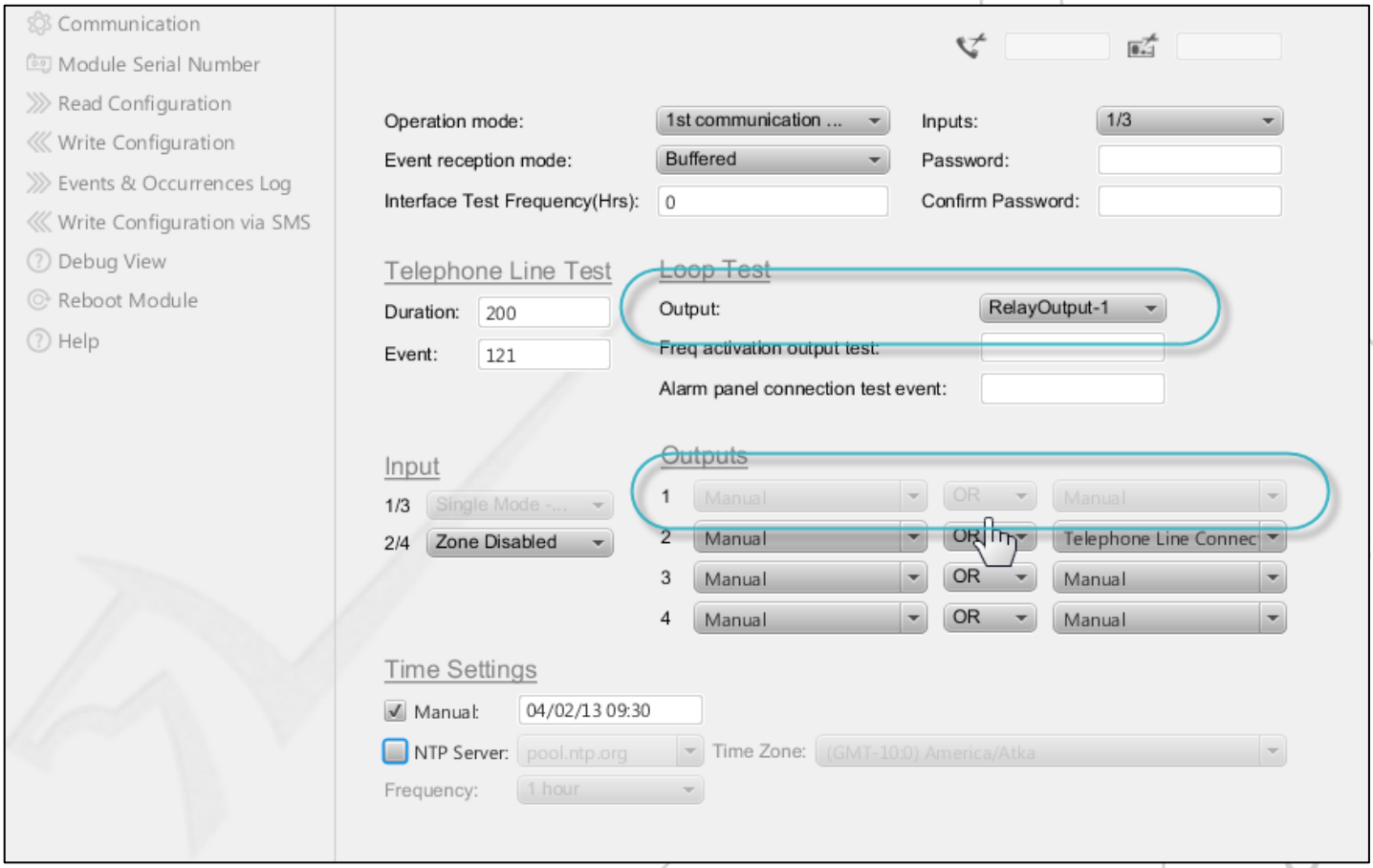


3. Under Outputs 2, select either the **OR** option or the **AND** option.



4. Likewise, you can select output options from **Outputs: 3 and 4**.

> **Note:**
>
> Here. **Output 1** drop-down boxes are in the disabled mode as **Relay Output -1** is already selected as an output for alarm panel loop test.

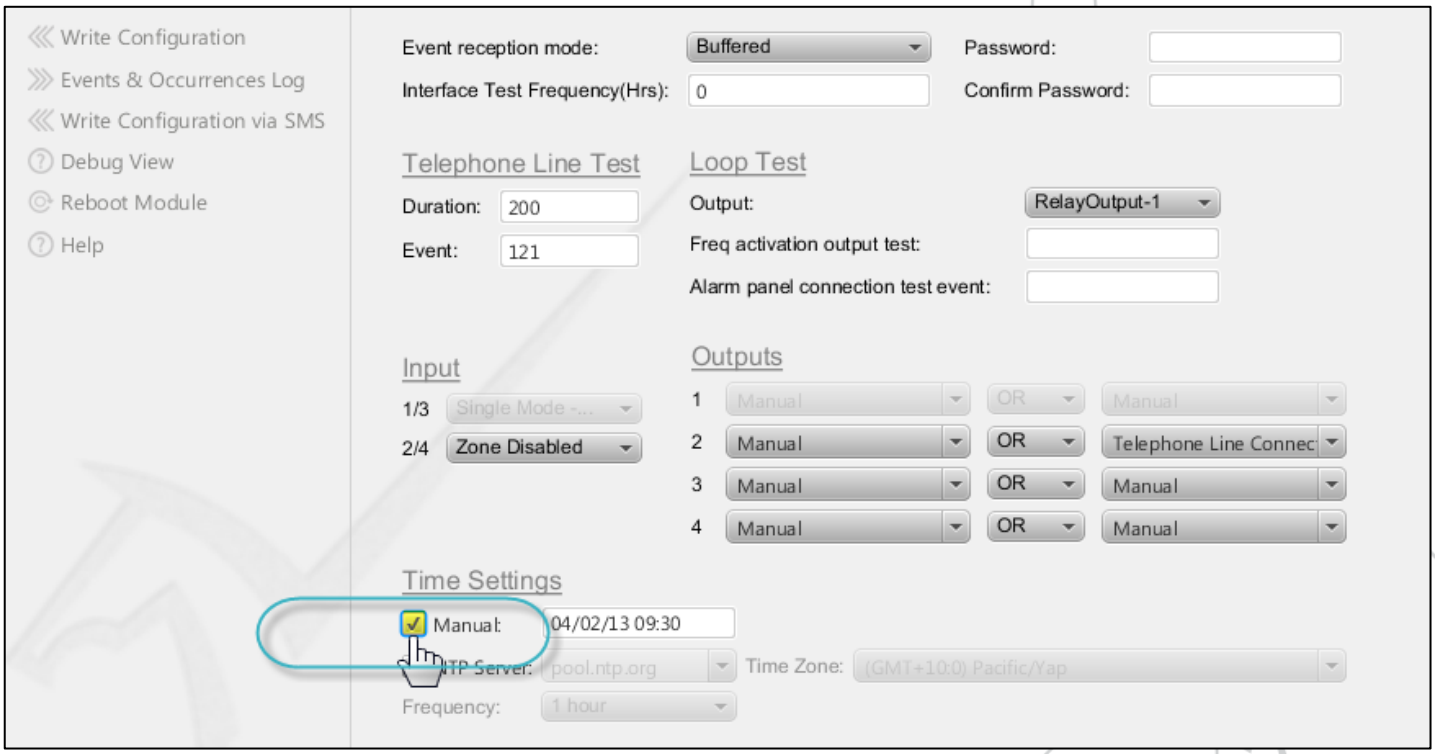


3.11. Configure Time Settings

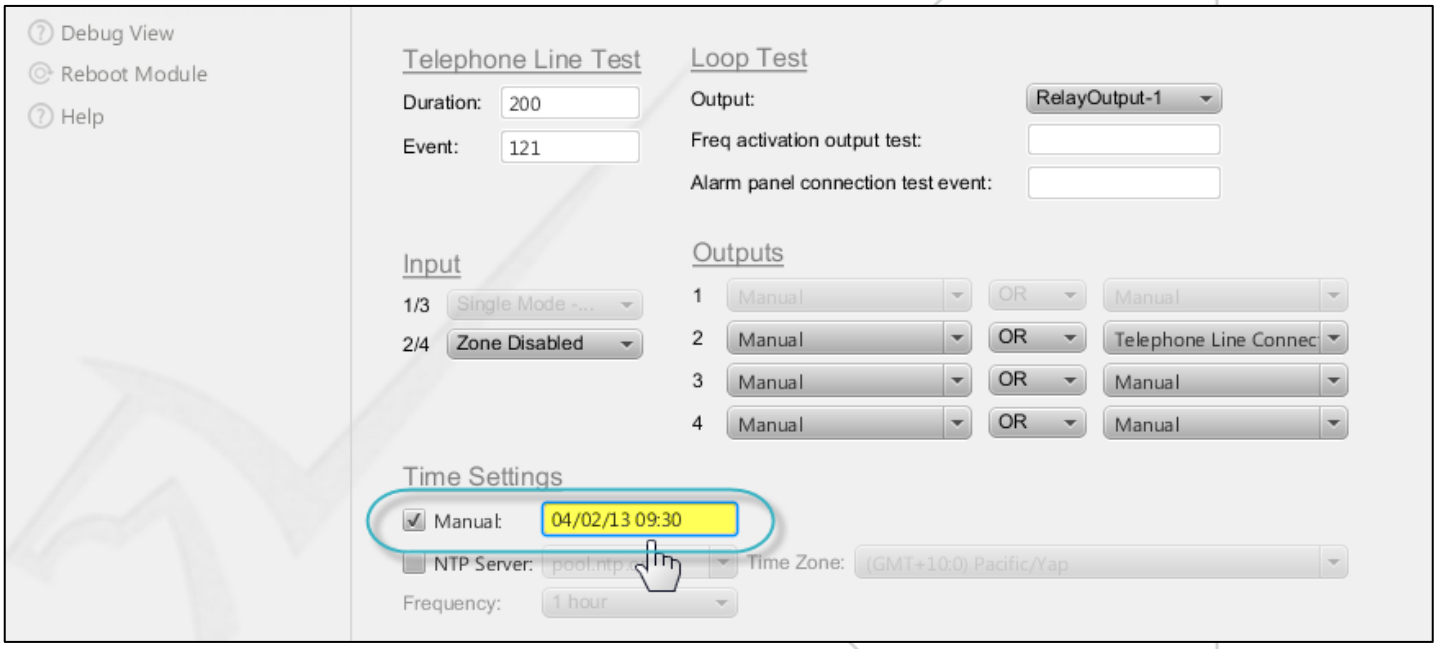
Pegasus NX supports time settings manually or by using the Network Time Protocol (NTP) server. NTP is a network protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. NTC provides Coordinated Universal Time (UTC) including scheduled leap second adjustments.

To configure time settings manually

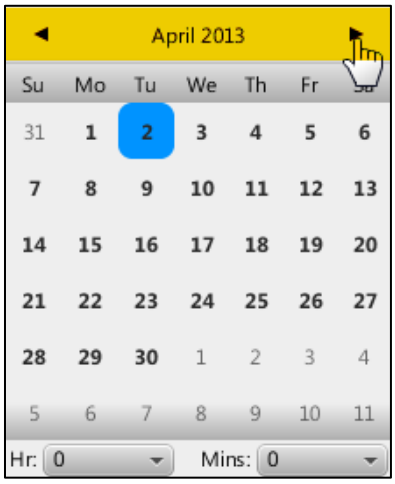
1. Select the **Manual** check box.



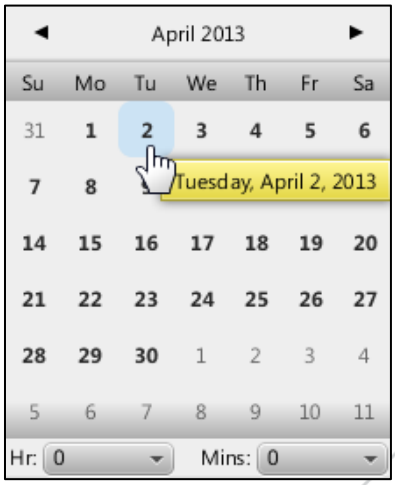
2. Click inside the **Manual** text box.



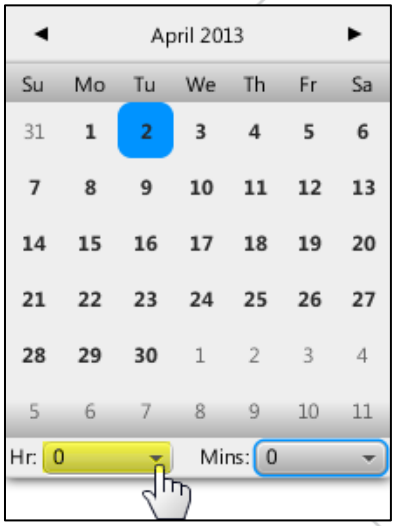
3. A pop-up box is displayed. Using the left/right arrow, select the current month and year.



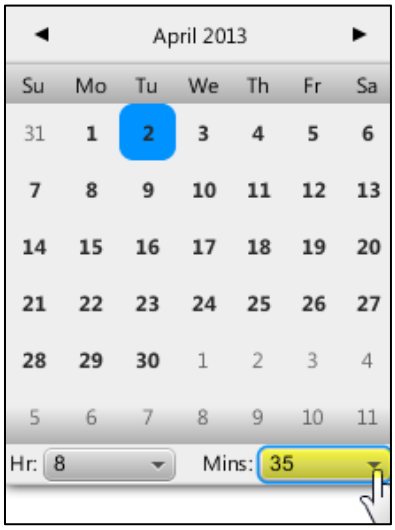
4. Select the **Current Date**.



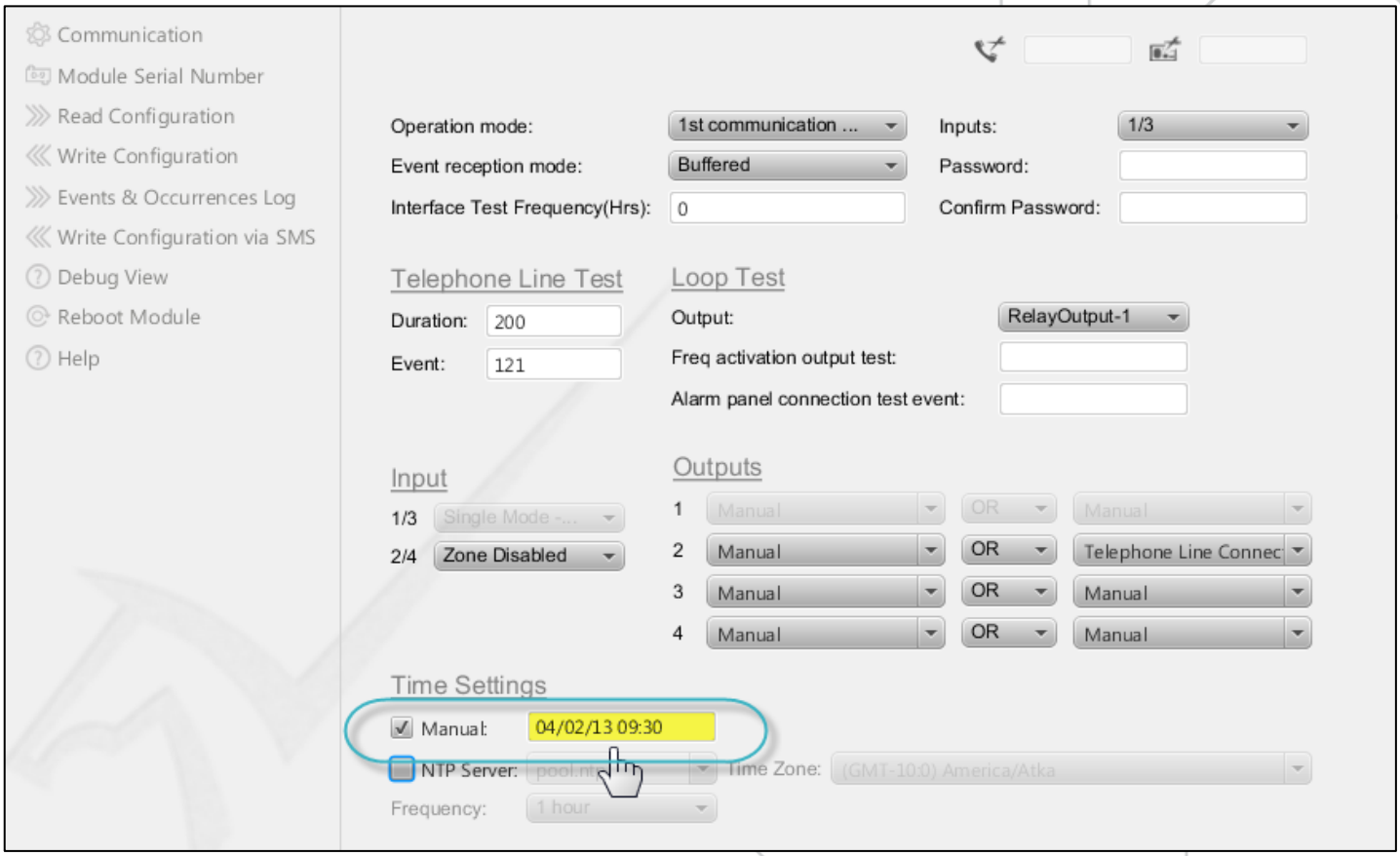
5. On the **Hr** menu, select **Duration in Hour(s)**.



6. On the **Mins** menu, select **Duration in Minutes.**

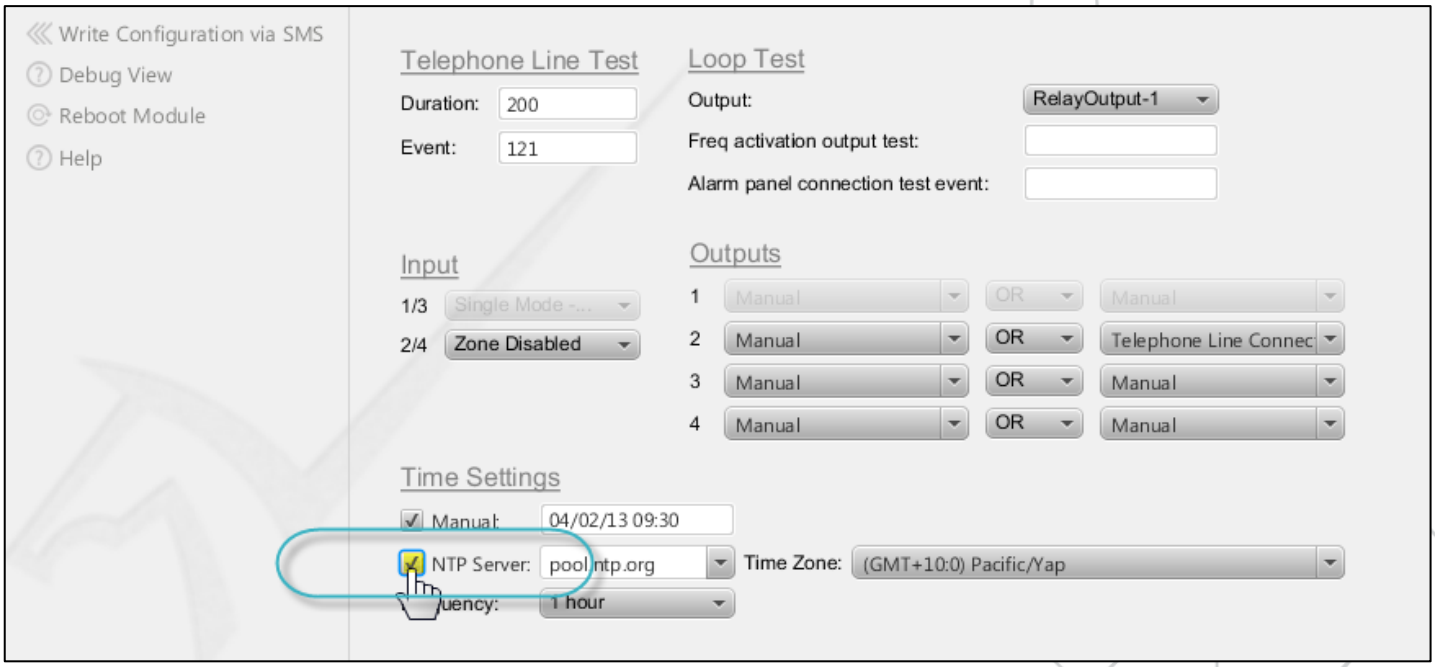


The configured time is displayed in the **Manual** text box.

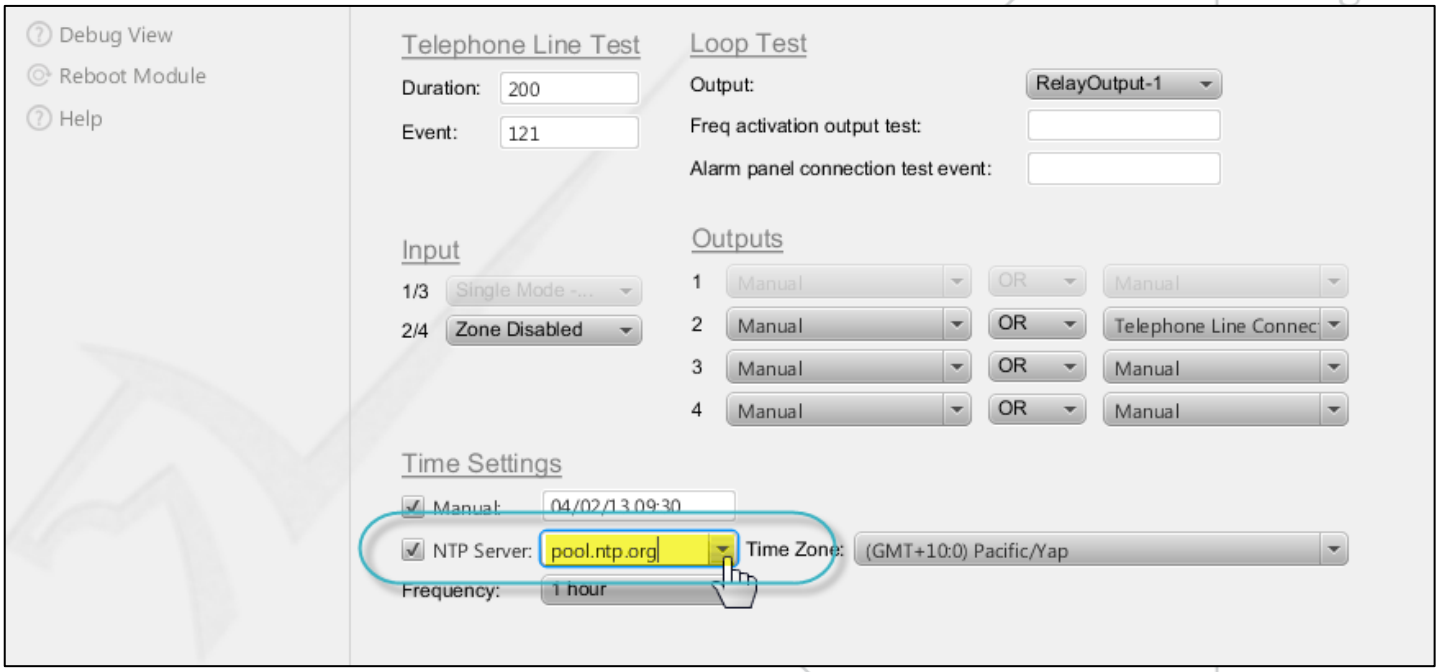


To configure time settings using the NTP server

1. Select the **NTP Server** check box.



2. In the **NTP Server** drop-down box, type-in the **NTP Pool Time Server Address.**

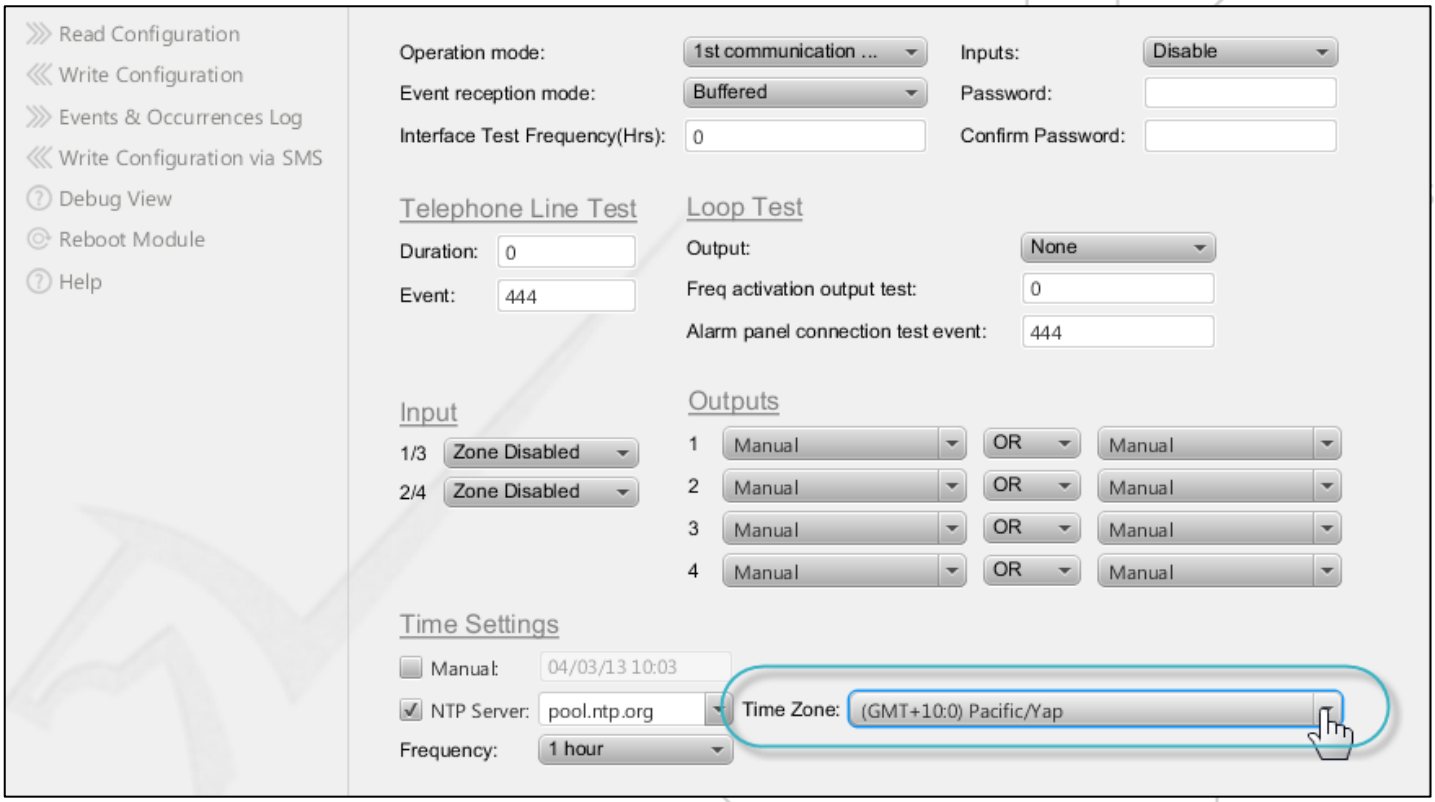


The NTP Pool DNS system automatically picks time servers which are geographically close for you, but if you want to choose explicitly, there are sub-zones of pool.ntp.org. The continent ones are:

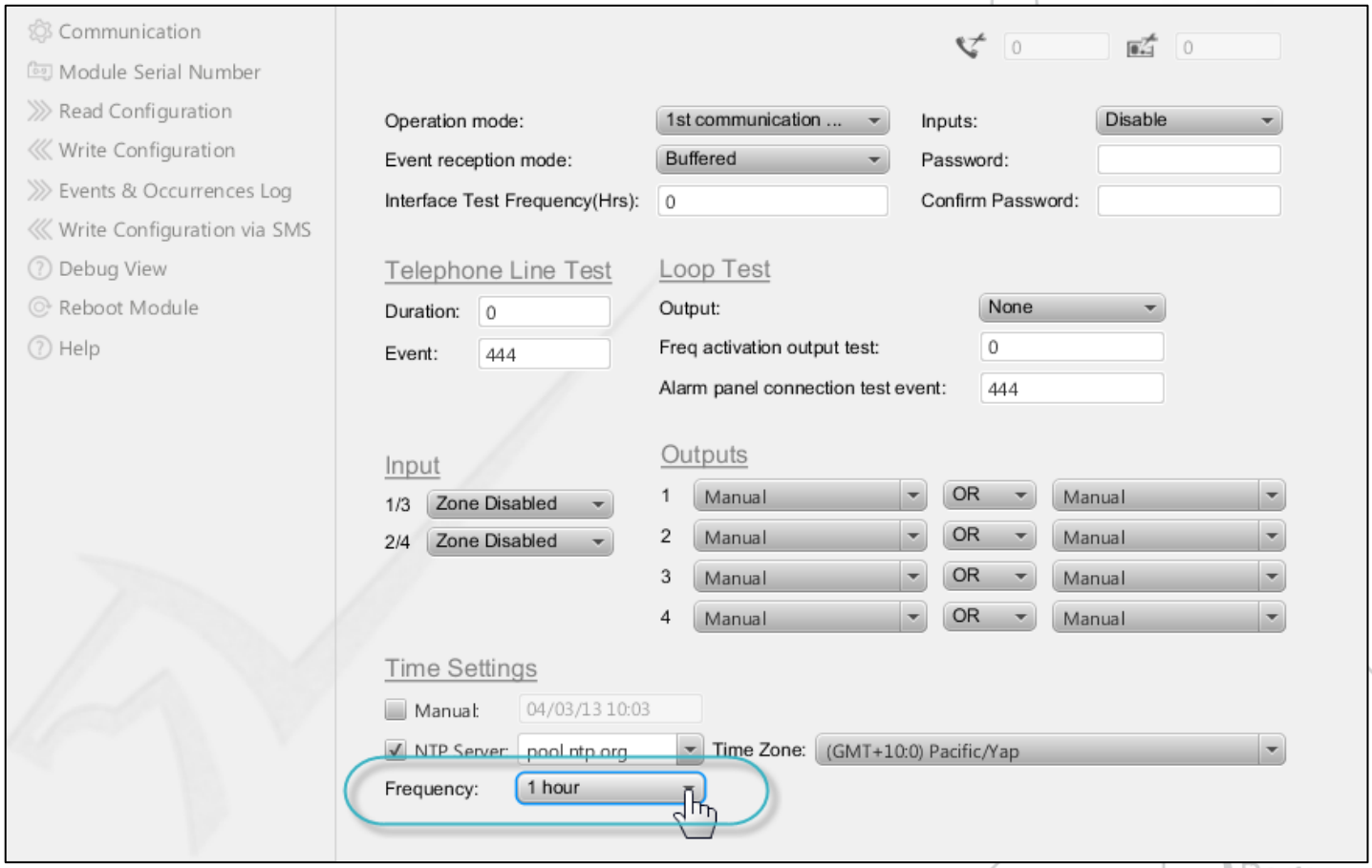
Important Information:

Area	Host Name
Worldwide	pool.ntp.org
Asia	asia.pool.ntp.org
Europe	europe.pool.ntp.org
North America	north-america.pool.ntp.org
Oceania	oceania.pool.ntp.org
South America	south-america.pool.ntp.org

3. In the **Time Zone** drop-down box, select the appropriate **Time Zone.**

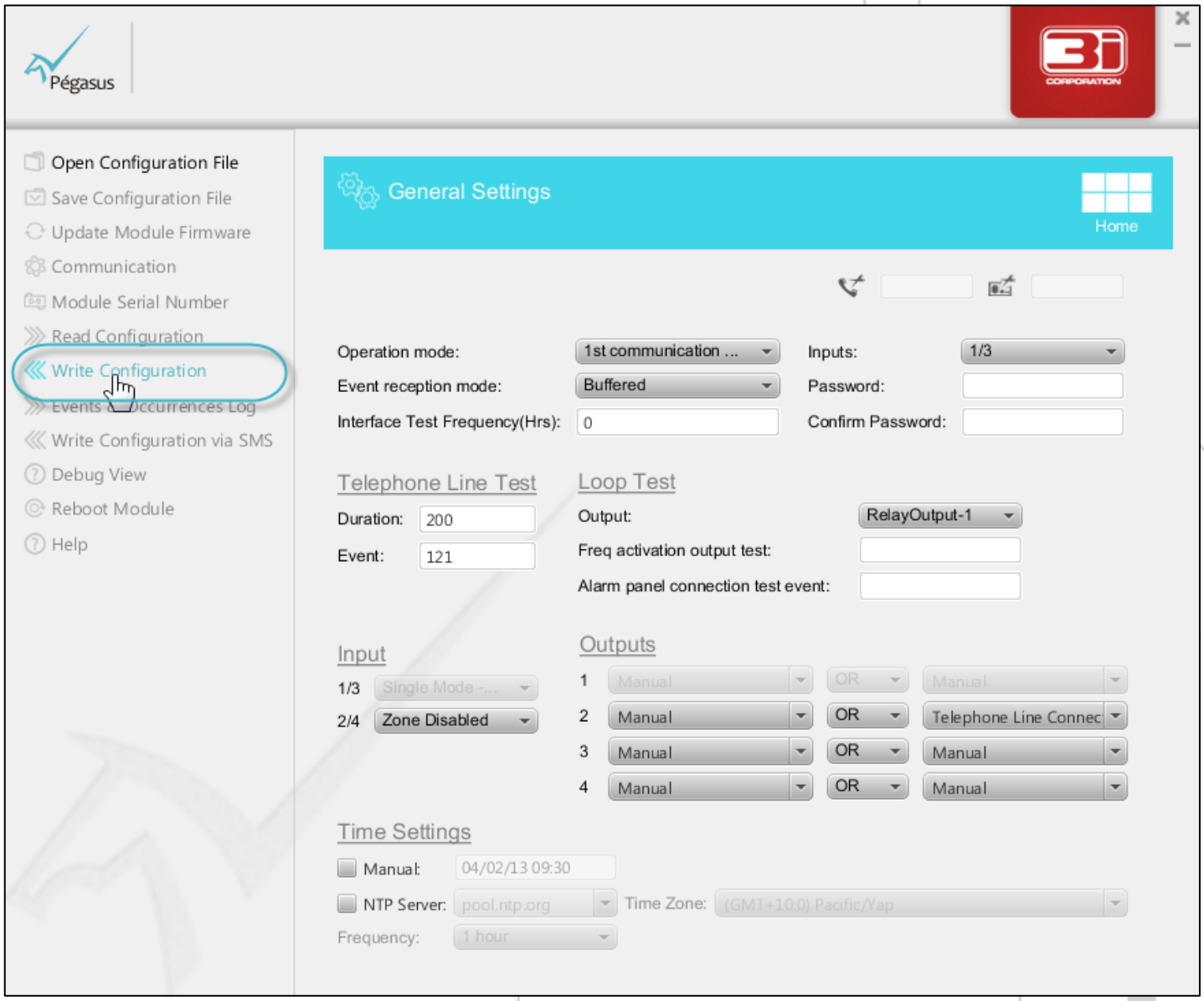


4. In the **Frequency** drop-down box, select the frequency of time update from the NTP Server**.** The available frequencies are: 1 hour, 12 hour, 1 day, 1 week, and 1 month.


Communication
Module Serial Number
Read Configuration
Write Configuration
Events & Occurrences Log
Write Configuration via SMS
Debug View
Reboot Module
Help
0
0
Operation mode:
1st communication ...
Inputs:
Disable
Event reception mode:
Buffered
Password:
Interface Test Frequency(Hrs):
0
Confirm Password:
Telephone Line Test
Duration:
0
Event:
444
Loop Test
Output:
None
Freq activation output test:
0
Alarm panel connection test event:
444
Input
1/3
Zone Disabled
2/4
Zone Disabled
Outputs
1
Manual
OR
Manual
2
Manual
OR
Manual
3
Manual
OR
Manual
4
Manual
OR
Manual
Time Settings
Manual:
04/03/13 10:03
NTP Server:
pool.ntp.org
Time Zone:
(GMT+10:0) Pacific/Yap
Frequency:
1 hour

3.12. Write Configuration

When the General Settings configuration is done, write the configuration settings to Pegasus™ NX.

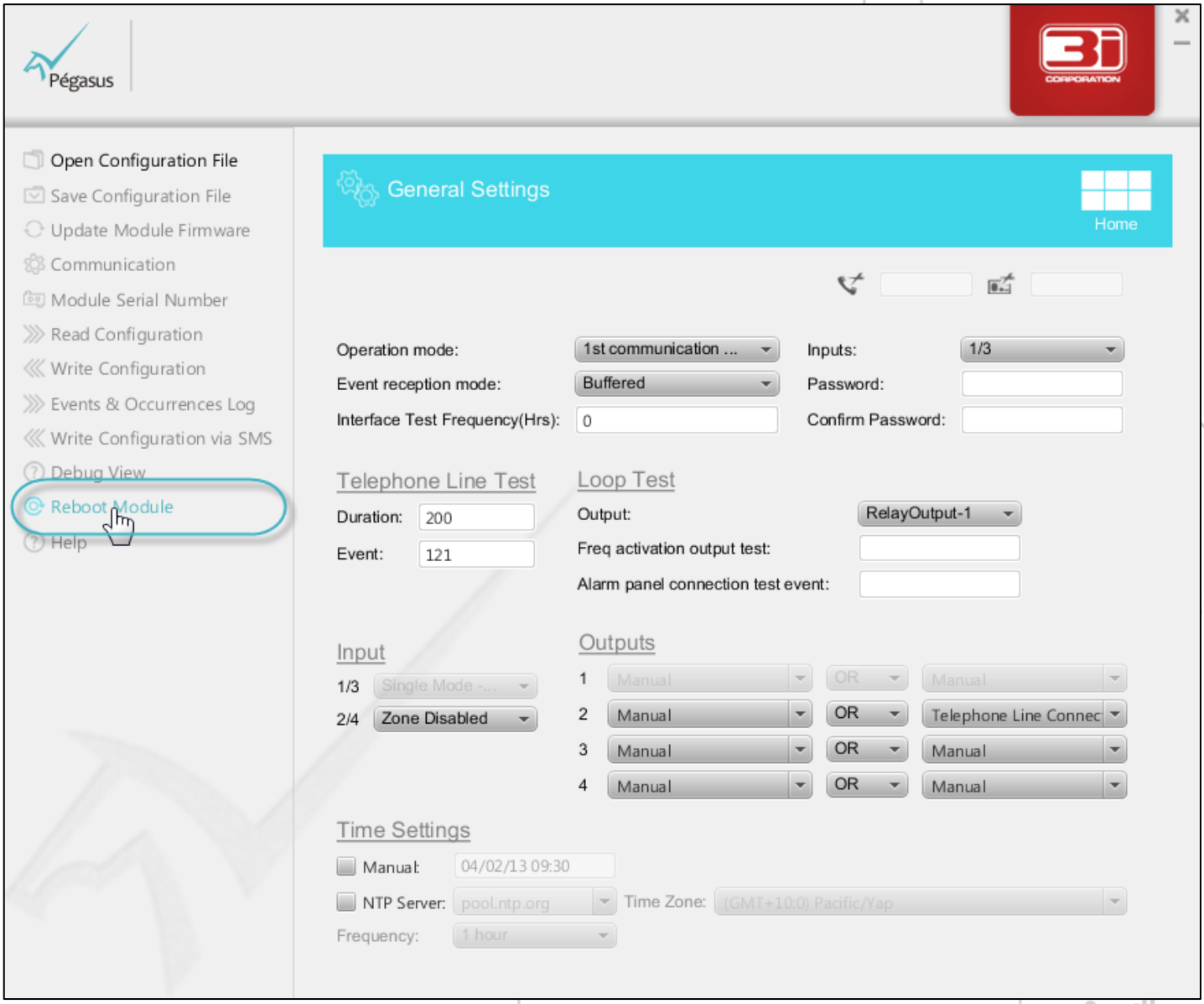


Note:

To learn how to write the configuration settings to Pegasus™ NX, refer the **Write Configuration** chapter.

3.13. Reboot Module

On successful writing of the Pegasus NX configfuration settings, to make all configured features functional, reboot of module is required.



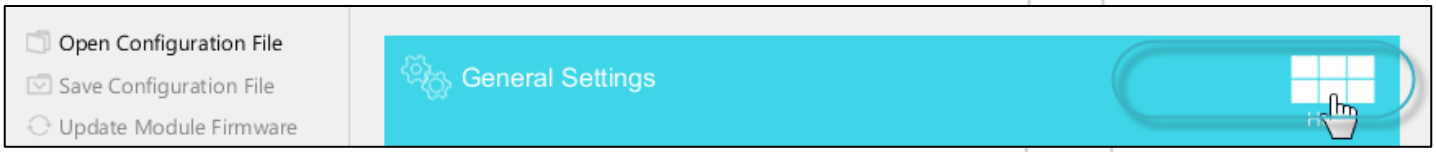
Note:

To learn how to reboot module after writing the configuration to Pegasus™ NX, refer the **Reboot Module** chapter.

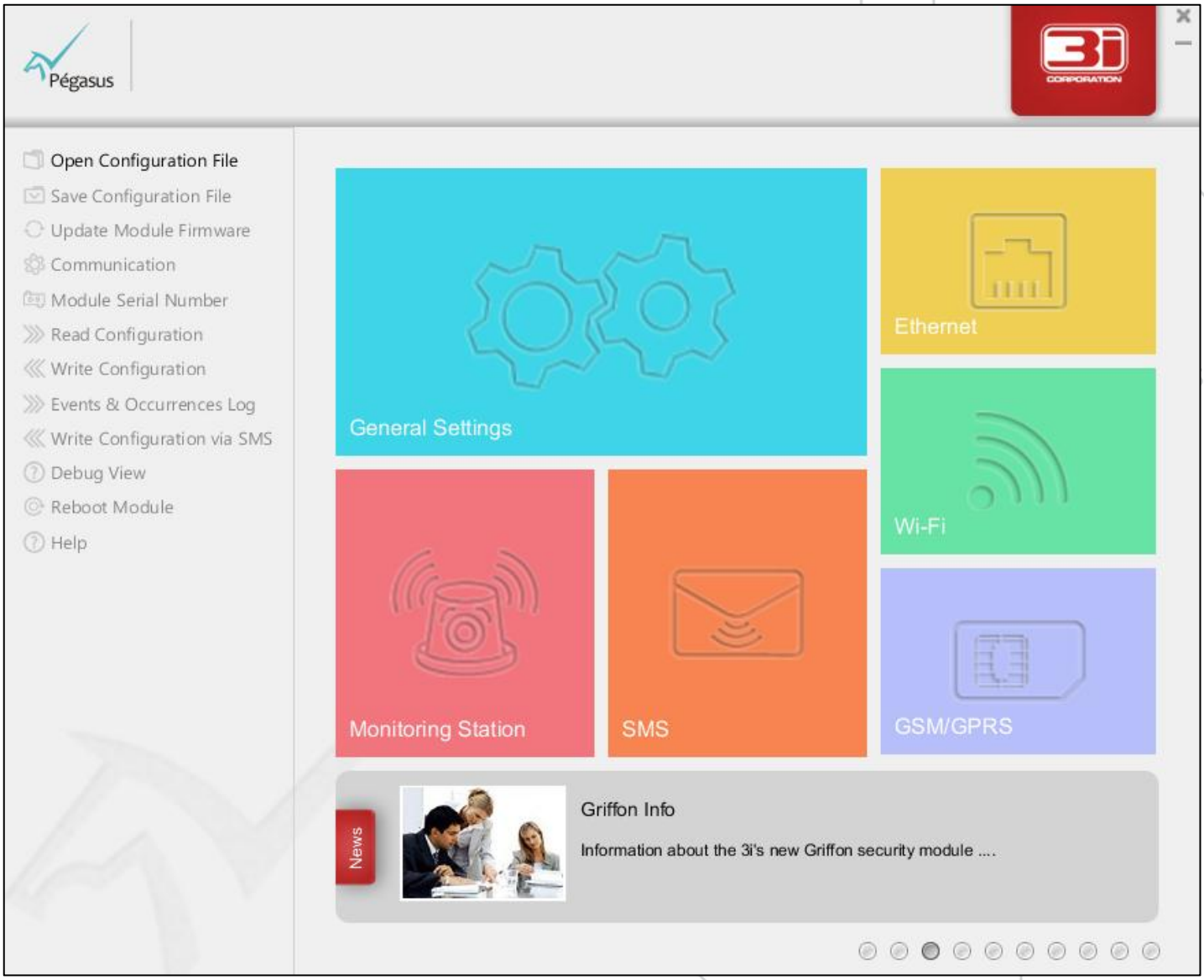
3.14. Return Back to Home Screen

To return back to the home screen

1. Click the **Home** icon as shown in the below image.



The **Pegasus™ Studio Home Screen** is displayed.



4 GSM/GPRS

The **GSM/GPRS** screen allows you to enable/disable, and configure all the parameters related to the GSM/GPRS interface available in Pegasus™ NX.

Configuration Instructions

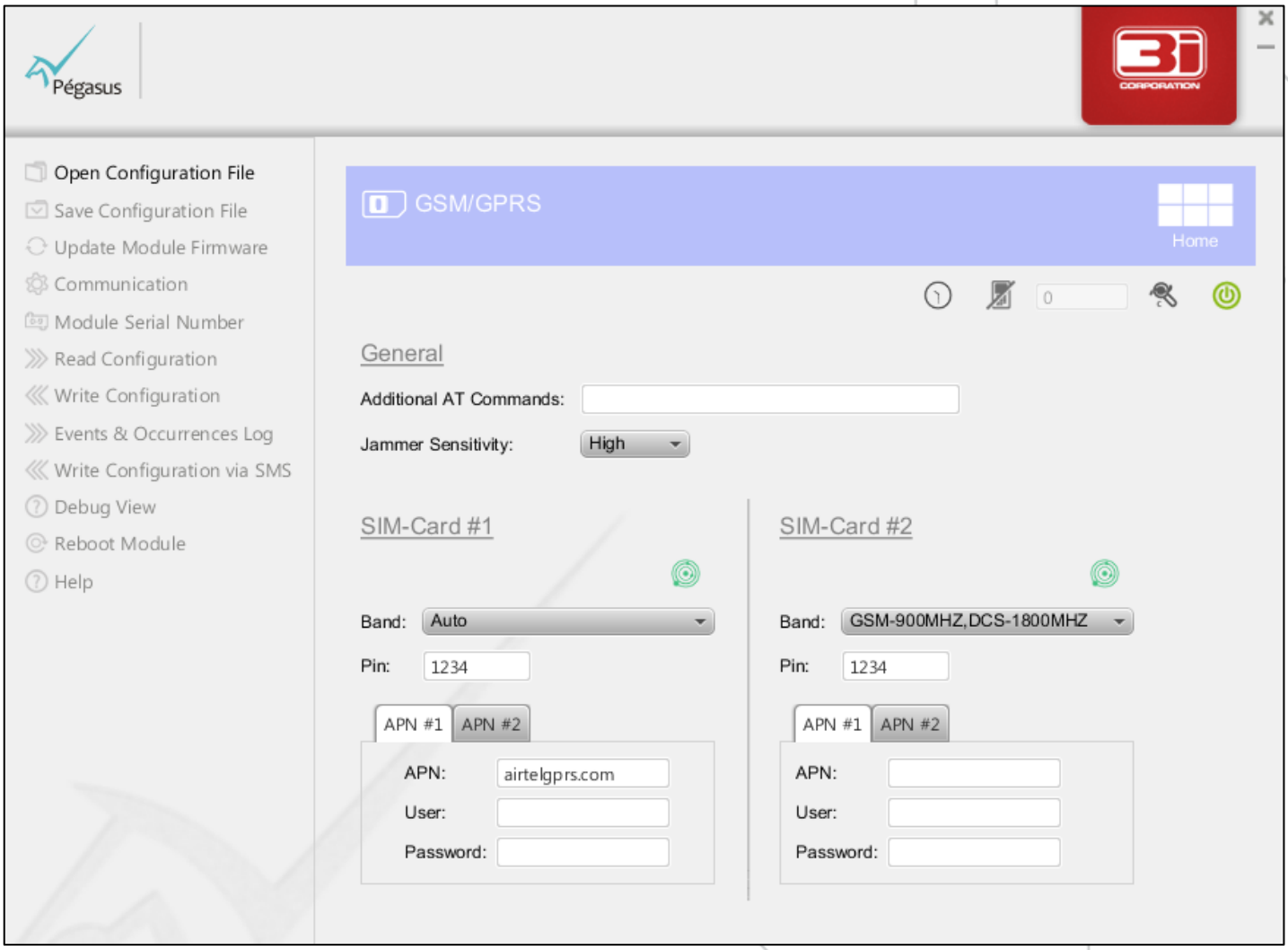
- To configure GSM/GPRS, follow steps: 4.1 to 4.10.
- To configure additional delay duration in the gsm jammer detection, follow steps: 4.3. Enable GSM Jammer, and 4.4. Configure Additional Delay Duration in the GSM Jammer Detection.
- To update the GSM modem firmware, follow step 4.7. Update Modem Firmware. This is an optional step.
- To write the GSM/GPRS configuration to Pegasus NX, follow step 4.8: Write Configuration. To apply the GSM/GPRS configuration settings, follow step 4.9: Reboot Module.

4.1. Open the GSM/GPRS Screen

To open the gsm/gprs screen

1. On the **Pegasus™ Studio Main Screen**, place your cursor on the **GSM/GPRS** section, and then click to open the **GSM/GPRS** screen.

The **GSM/GPRS** screen is displayed as shown below.



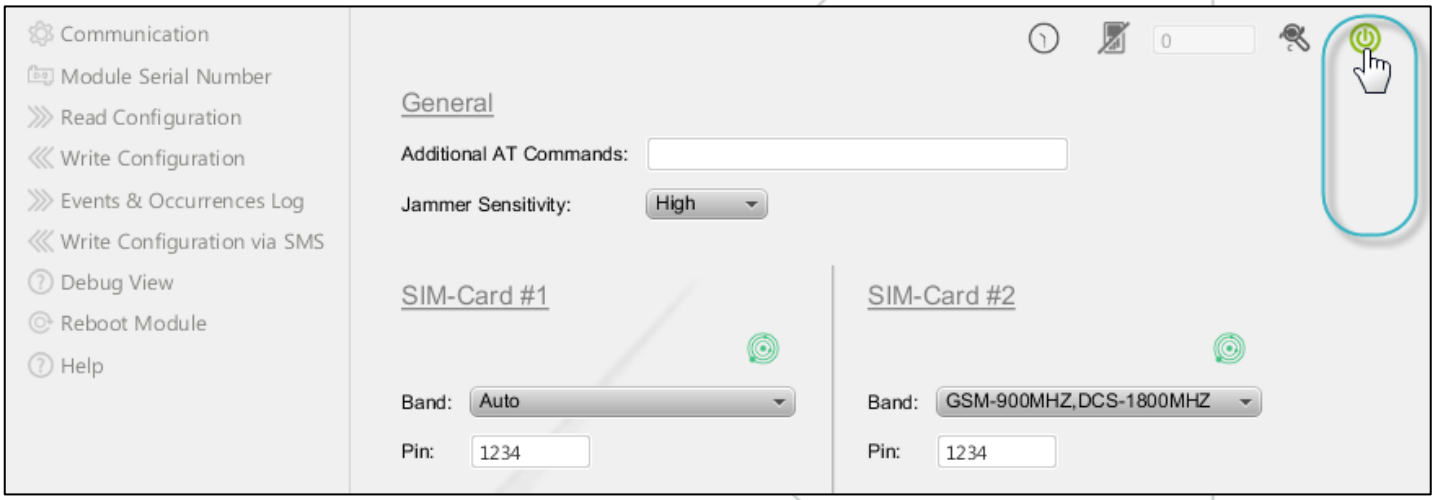
4.2. Enable the GSM/GPRS Interface

To perform the GSM/GPRS related configuration, it is required to enable the GSM/GPRS interface. Until the GSM/GPRS interface is enabled, all the fields and options in the GSM/GPRS screen are in the disabled state.

To enable the gsm/gprs interface

1. Click the grey colored **Enable GSM/GPRS**  icon.

The grey colored icon is turned green  as shown in the below image. The GSM/GPRS interface is in the enabled state.



4.3. Enable GSM Jammer

GSM Jammer when enabled allows you to identify active jamming of the GSM/GPRS network. This feature helps to prevent intruders that use GSM jammers to interfere with the normal network operation of Pegasus™ NX. Enabling the GSM Jammer is not mandatory.

To enable gsm jammer

1. Click the grey colored **GSM Jammer**  icon. The grey colored icon is turned green  as shown in the below image. The GSM Jammer is in the enabled state.

Once the GSM Jamer is enabled, the GSM/GPRS interface permits you to enter Additional Delay Duration in GSM Jammer Detection.

4.4. Configure Additional Delay Duration in the GSM Jammer Detection

To configure additional delay duration in the gsm jammer detection

1. In the **GSM Jammer** text box, enter the **Additional Delay Duration in GSM Jammer Detection** in seconds as shown in the below image.

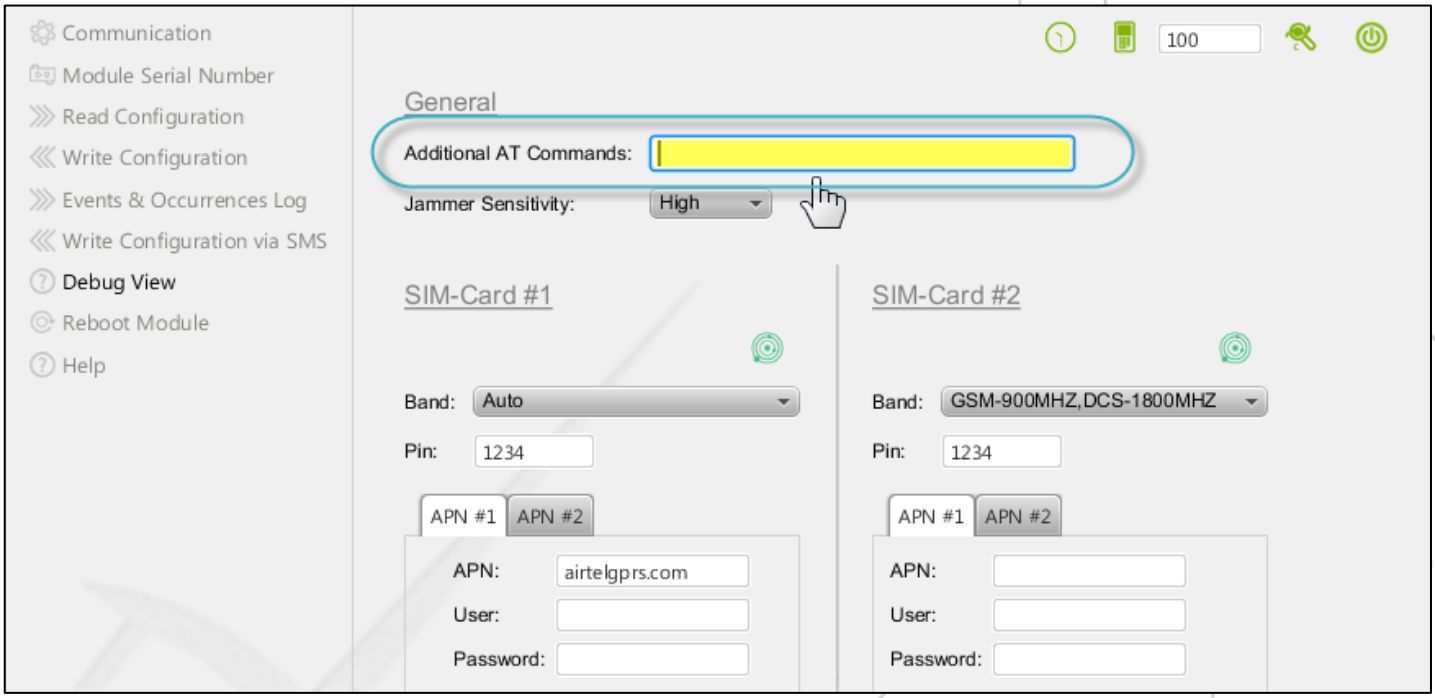
   The minimum acceptable duration is 0 second and the maximum acceptable duration is 300 seconds. The default duration is 0 second.

4.5. Configure General GSM/GPRS Settings

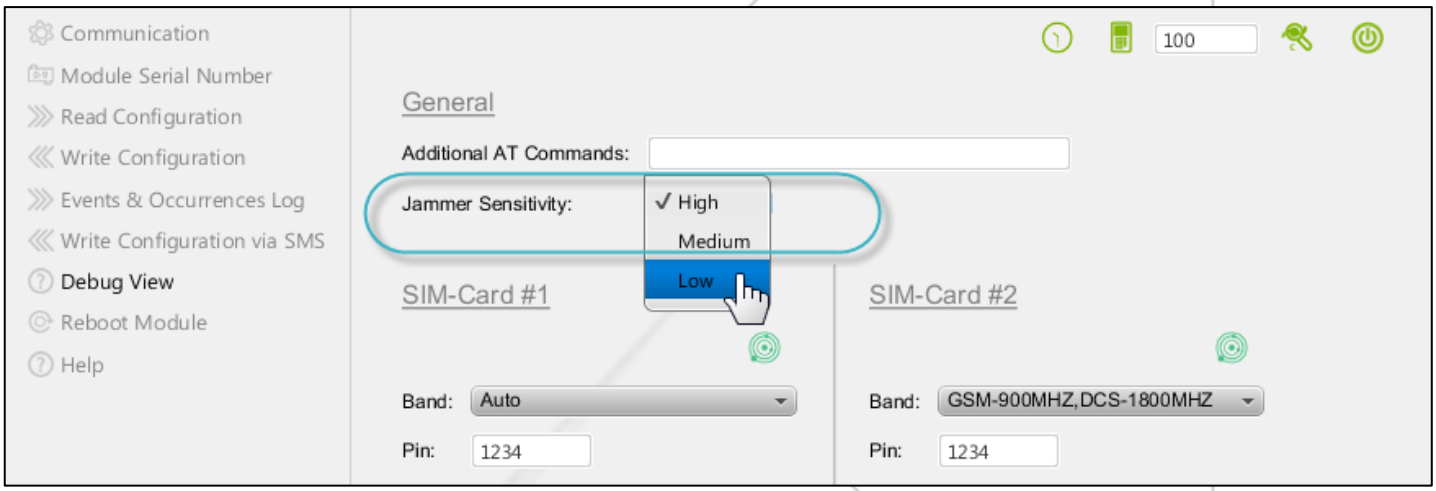
This section permits you to configure: Additional AT Commands and Jammer Sensitivity.

To configure general gsm/gprs settings

1. In the **Additional AT Commands** text box, enter an **AT command**. You can enter multiple AT commands separated by a semi-colon.



2. In the **Jammer Sensitivity** drop-down box, select the Jammer Sensitivity as **High** for long distance or **Medium** for intermediate distance or **Low** for close distance.



4.6. Configure SIM Cards

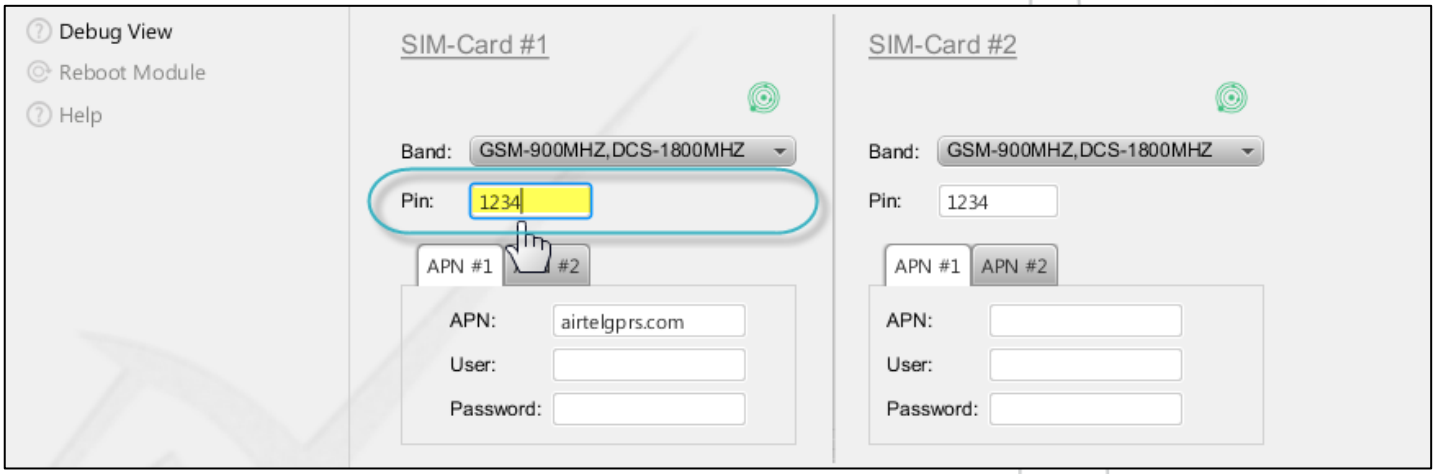
Pegasus™ NX is built-in dual SIM Cards. To use the GSM/GPRS functionality in the device, configuration of SIM Cards is required.

To configure sim cards

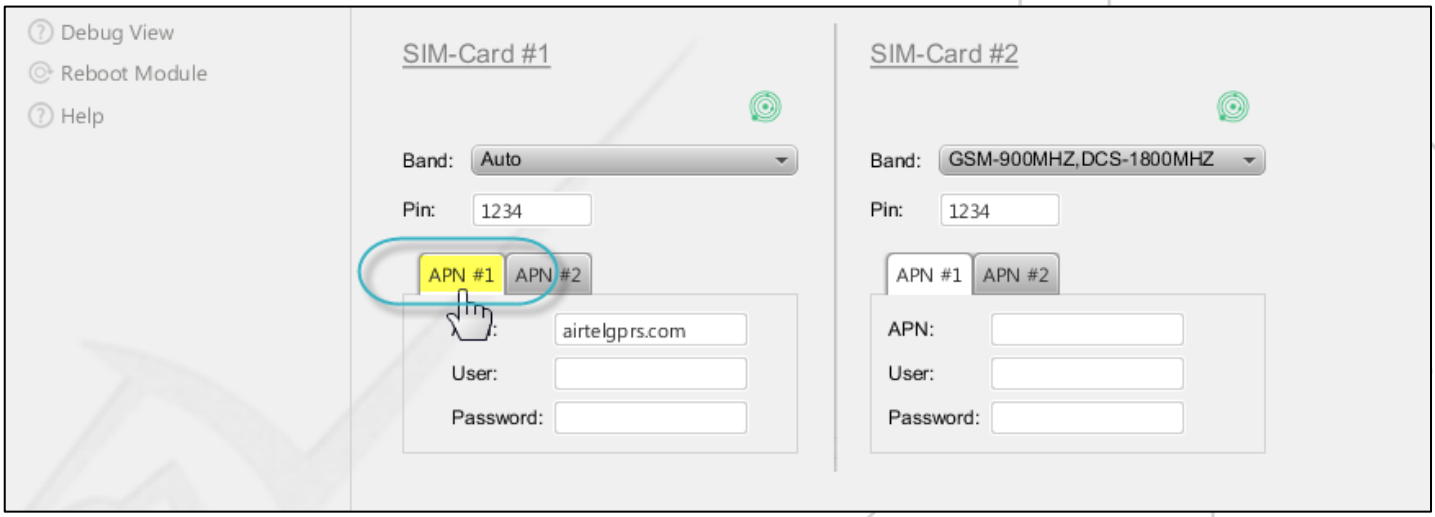
1. Under SIM-Card #1, in the **Band** drop-down box, select a **GSM Band.** You can also select the **Auto** option.

> **Additional Information:**
> For more information on GSM bands, see Appendix A: GSM Bands.

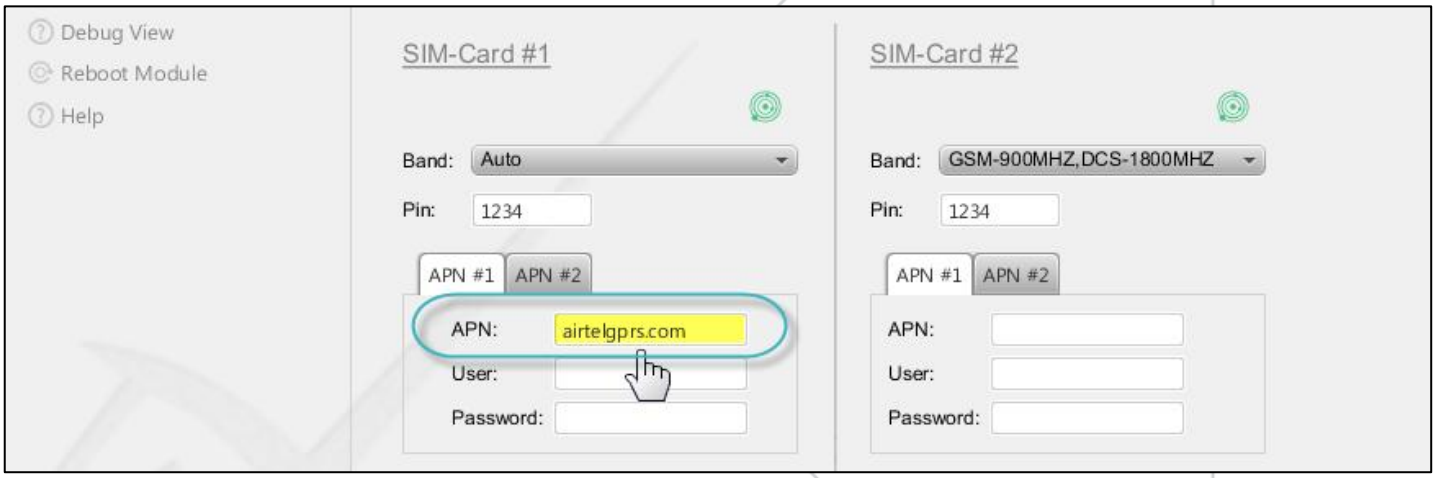
2. In the **Pin** text box, enter **SIM Card #1 PIN** provided by the GSM service provider.



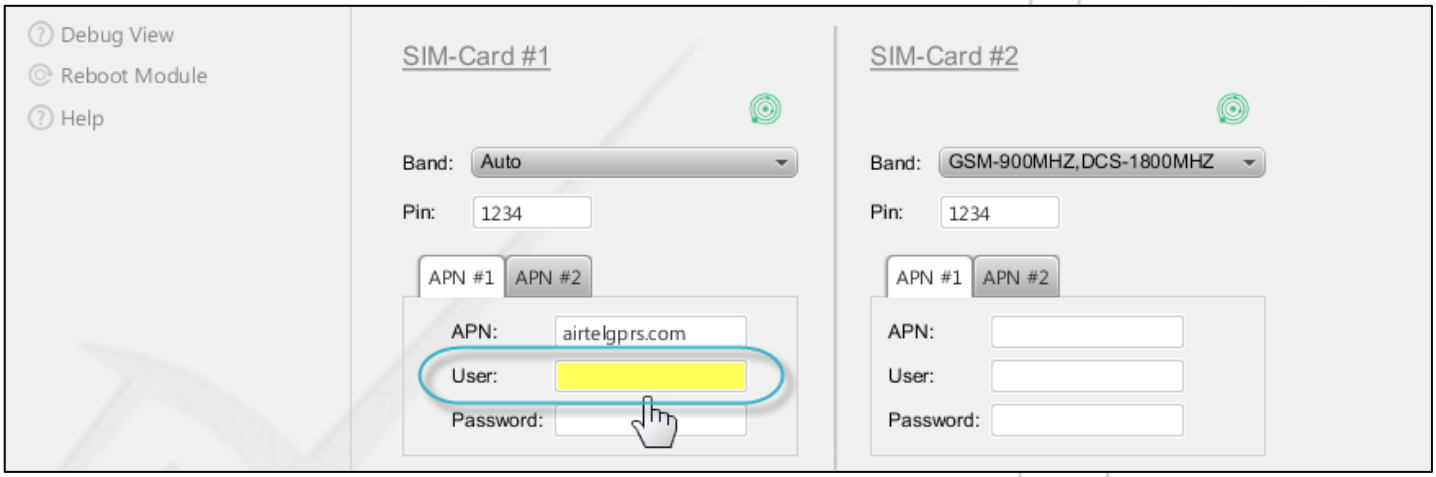
3. To enter the APN #1 configuration for SIM Card #1, click the **APN #1** tab.



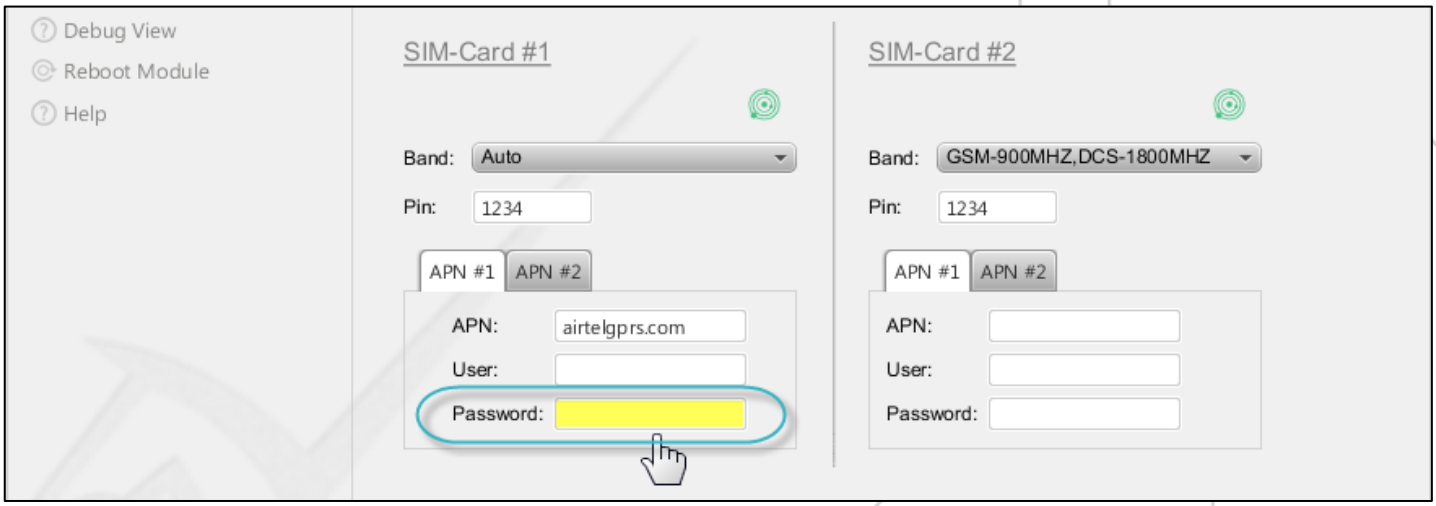
4. In the **APN** text box, enter the **Access Point Name** provided by the GSM service provider.



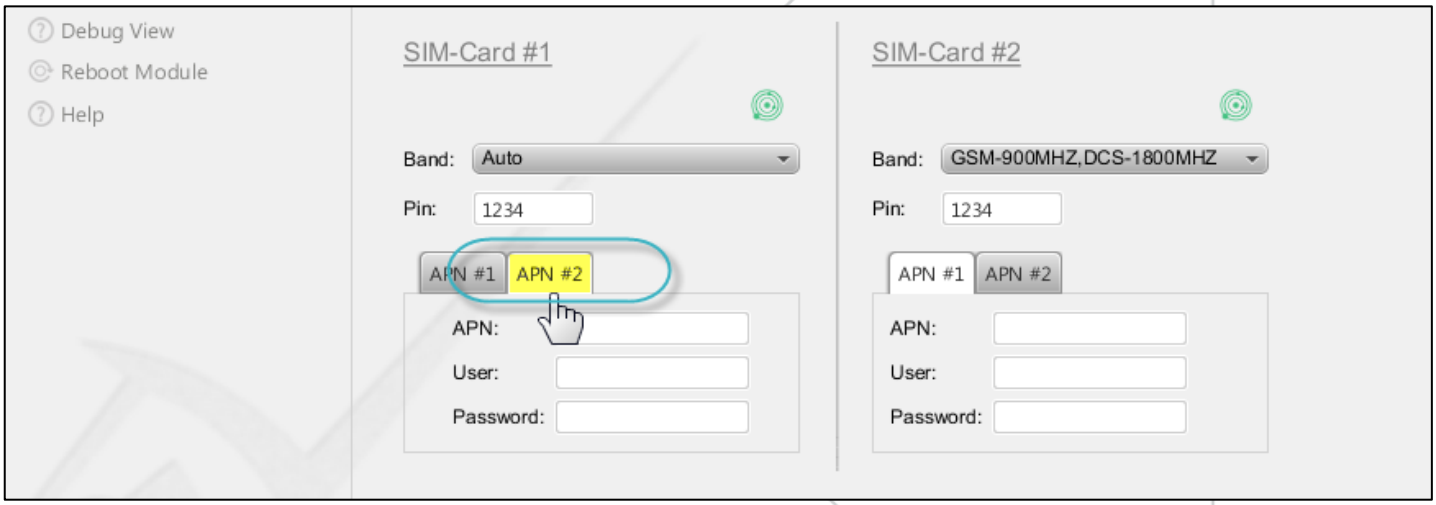
5. In the **User** text box, enter your **Username** provide by the GSM service provider.



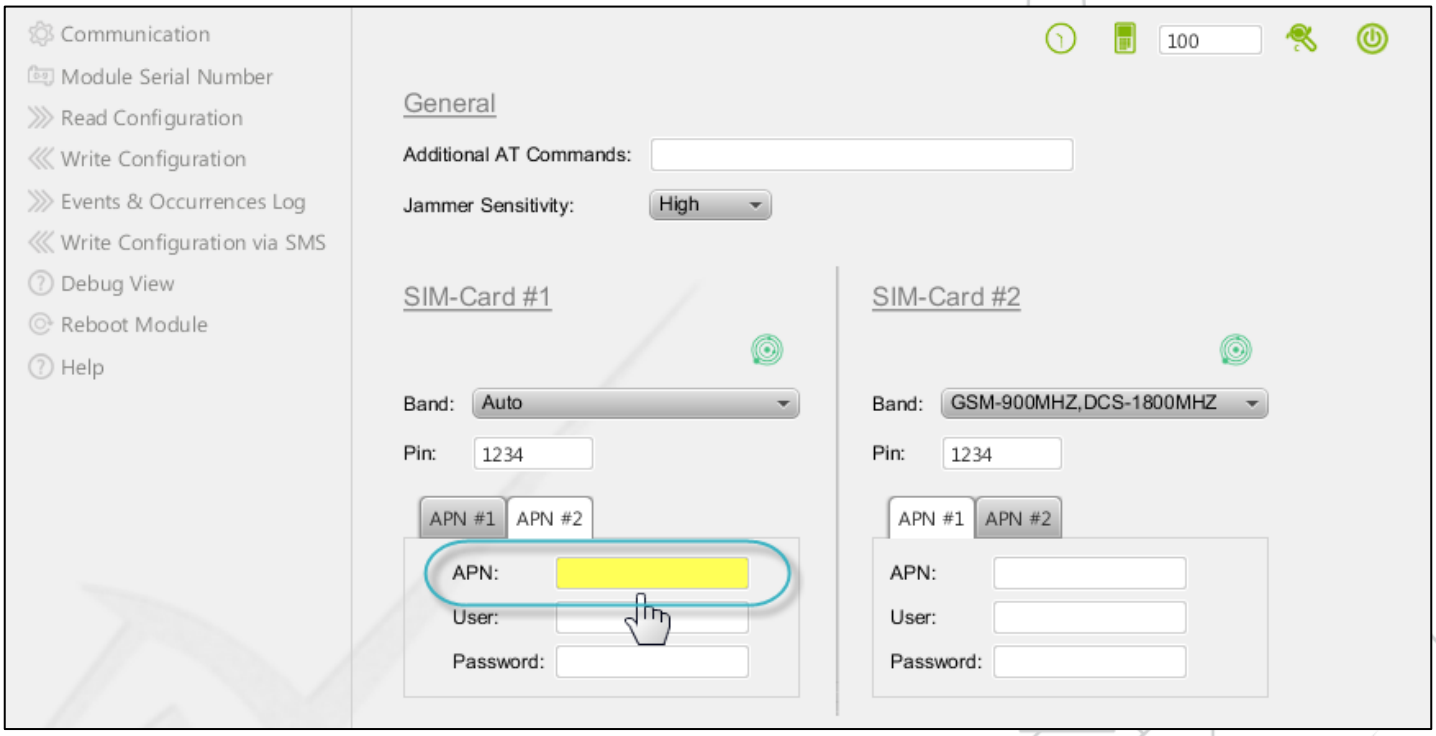
6. In the **Password** text box, enter your **Password** provided by the GSM service provider.



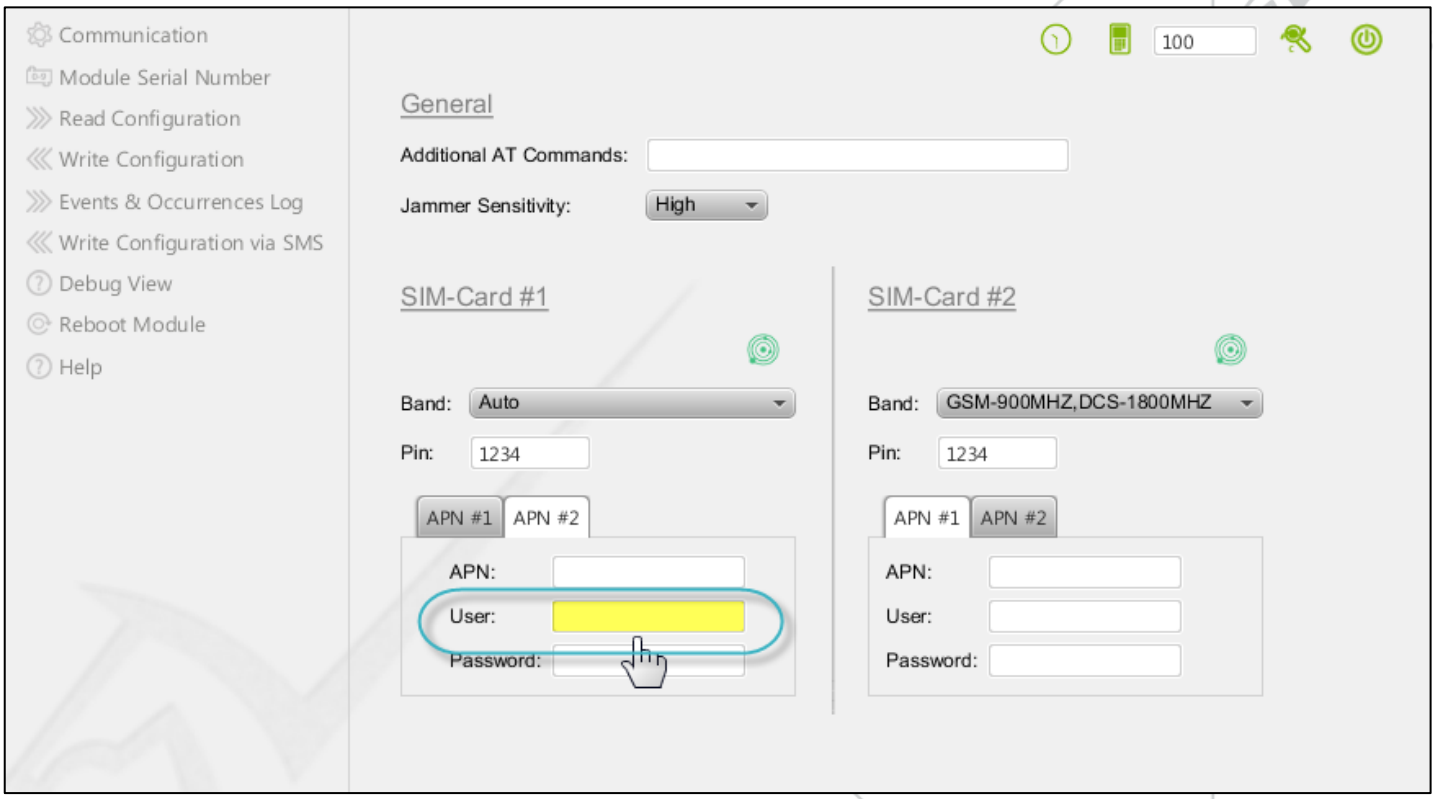
7. To enter the APN #2 configuration for SIM Card #1, click the **APN #2** tab.



8. In the **APN** text box, enter the **Access Point Name** provided by the GSM service provider.



9. In the **User** text box, enter your **Username** provide by the GSM service provider.



10. In the **Password** text box, enter your **Password** provided by the GSM service provider.

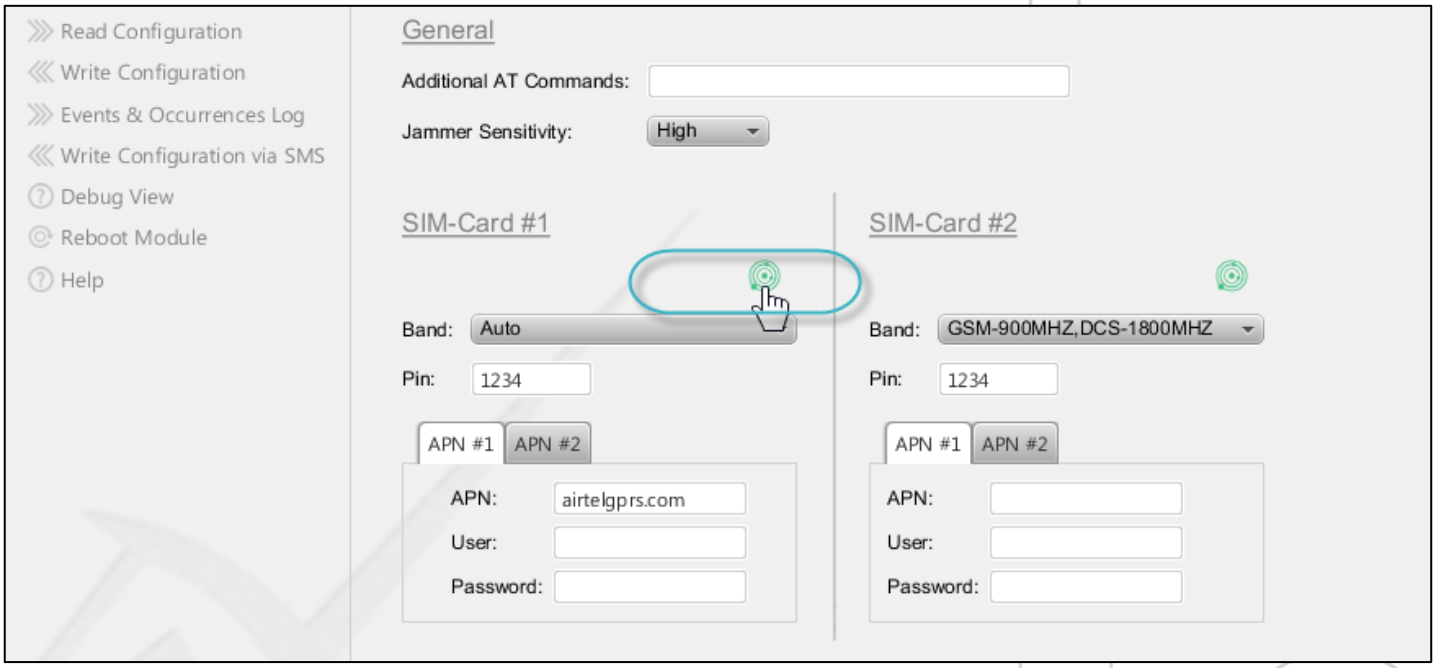
11. Likewise, you can configure SIM Card #2.

4.7. Update Modem Firmware (Optional)

Pegasus™ NX is FOTA capable, firmware updates are issued directly over-the–air from the GSM service provider to the GSM modem.

To update gsm modem firmware

1. Under SIM-Card #1, click **Firmware Update Over-the-Air**  icon.

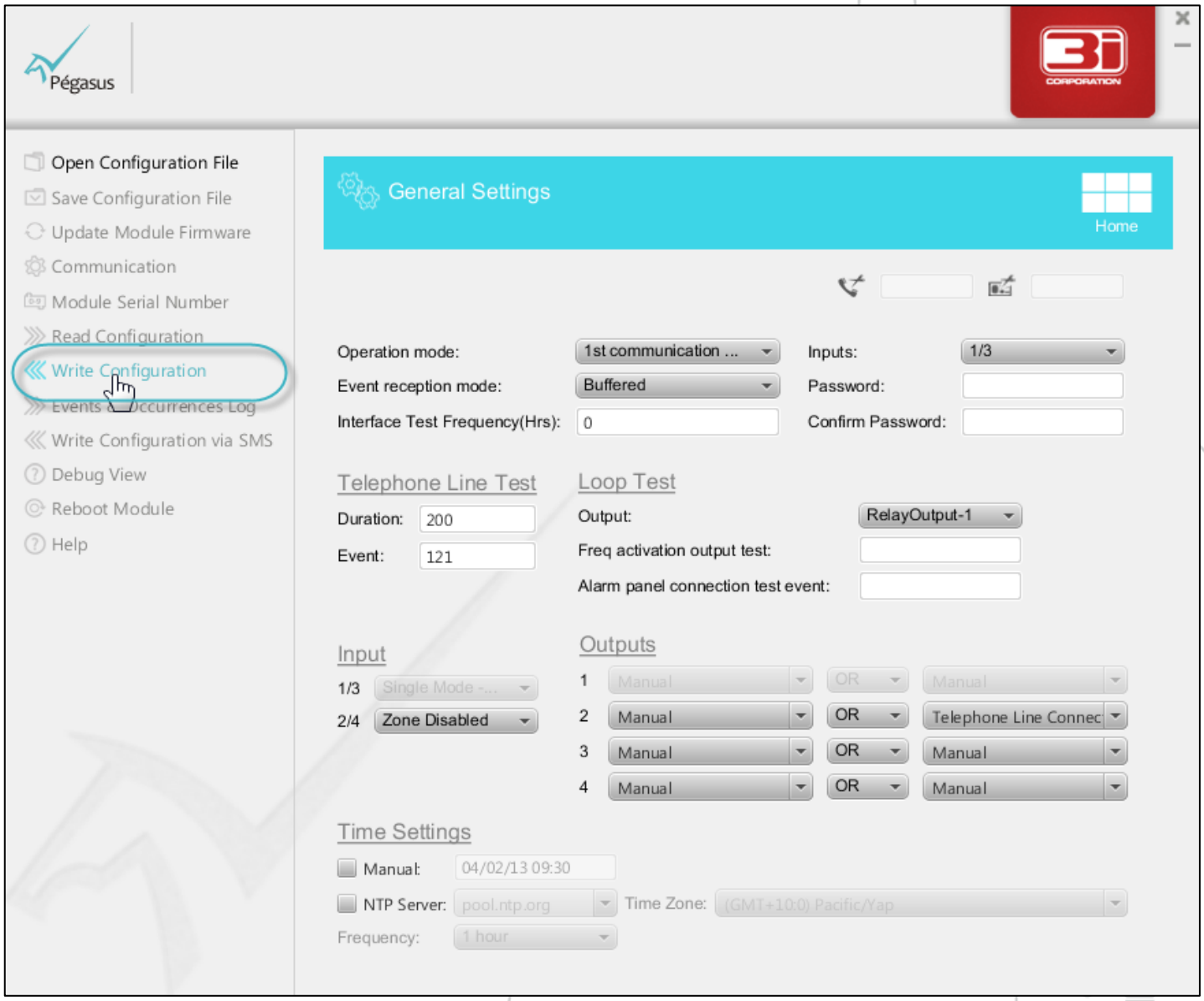


A message box is displayed saying, “Do You Want To Update SIM #1 GSM Firmware?”

2. Click the **Yes** button.

4.8. Write Configuration

When the GSM/GPRS configuration is done, write the configuration settings to Pegasus™ NX.

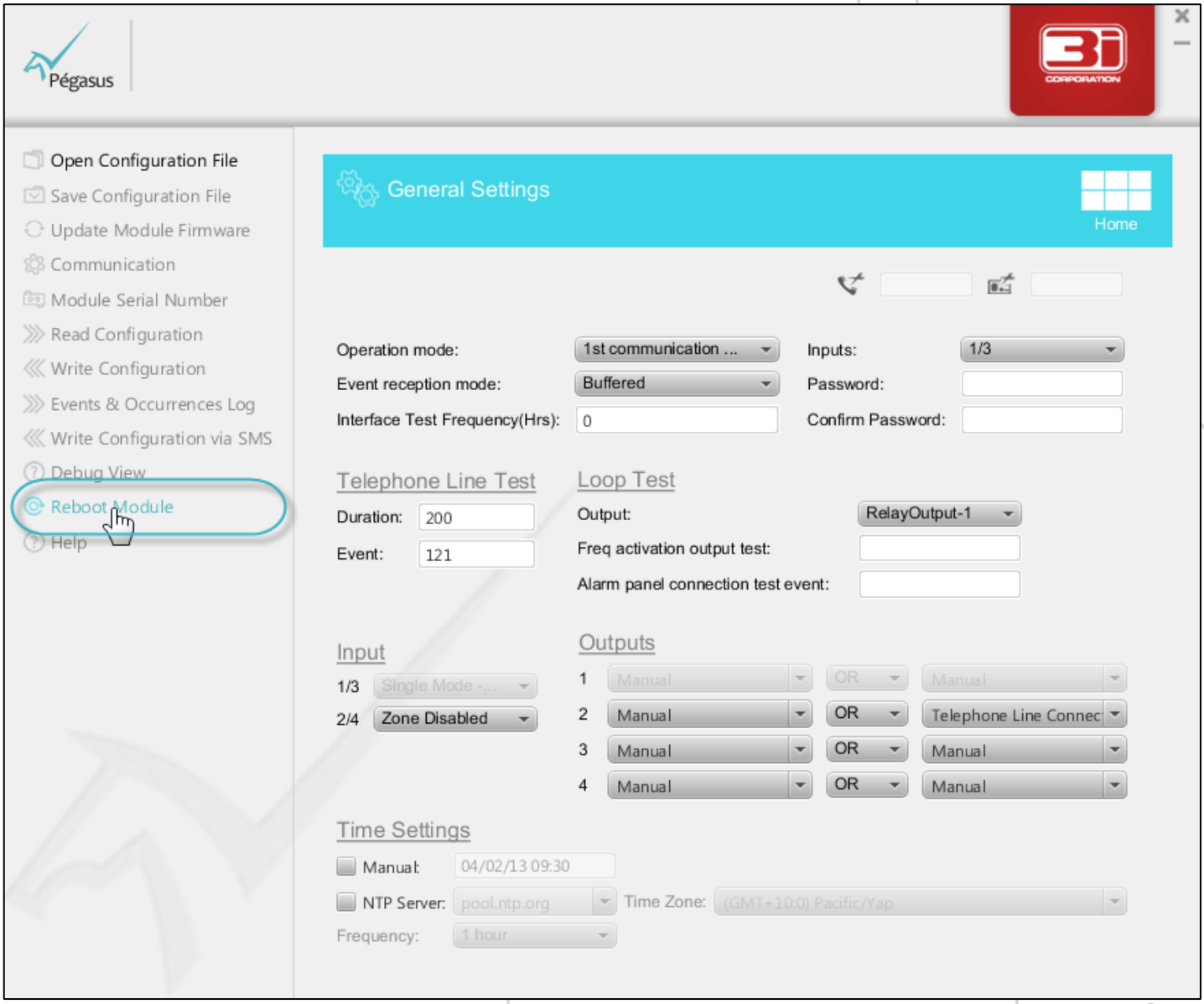


Note:

To learn how to write the configuration settings to Pegasus™ NX, refer the **Write Configuration** chapter.

4.9. Reboot Module

On successful writing of the Pegasus NX configfuration settings, to make all configured features functional, reboot of module is required.



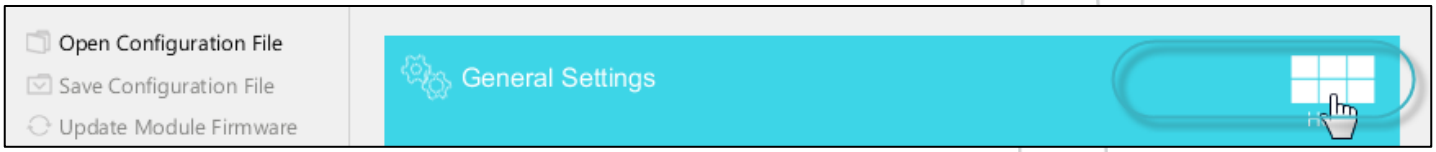
Note:

To learn how to reboot module after writing the configuration to Pegasus™ NX, refer the **Reboot Module** chapter.

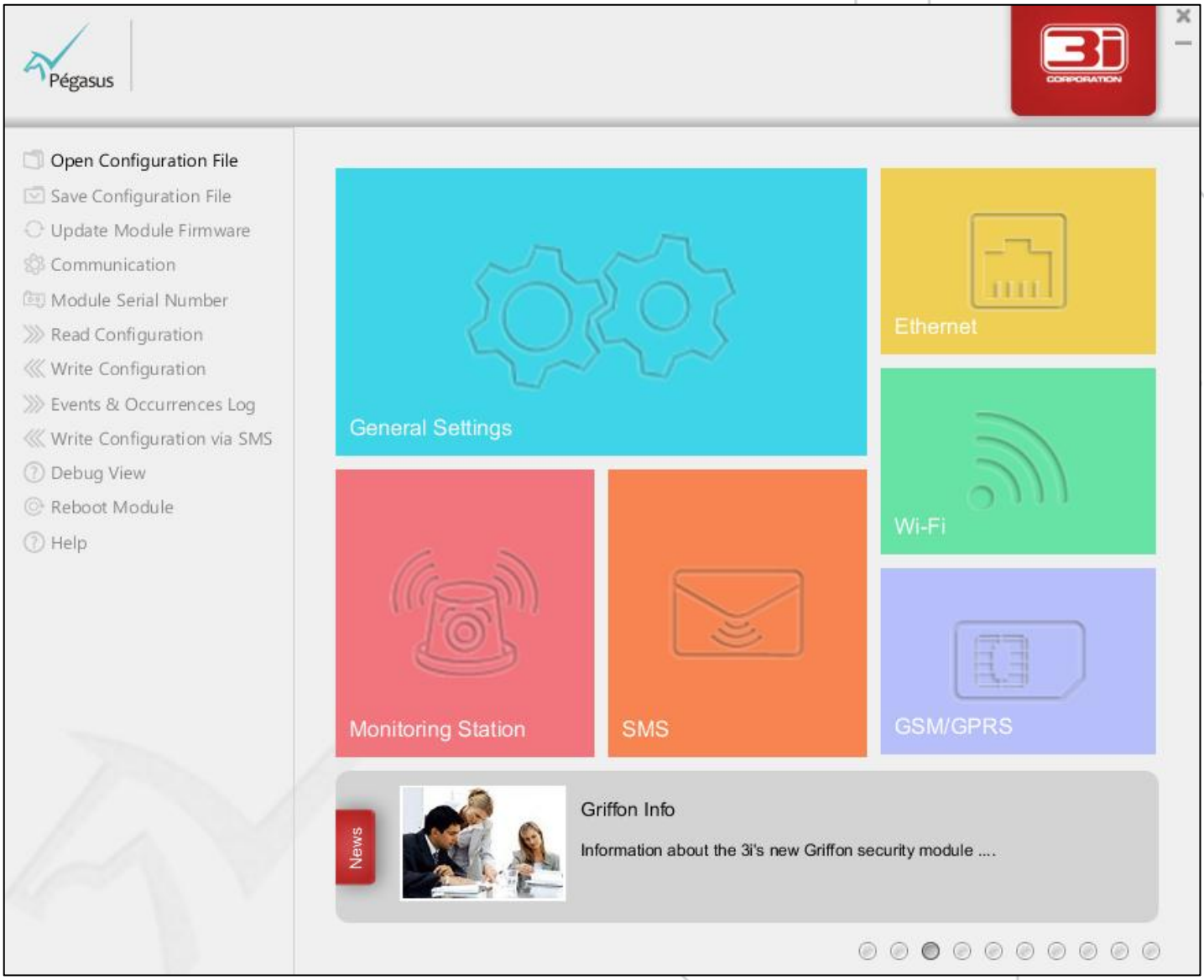
4.10. Return Back to Home Screen

To return back to the home screen

1. Click the **Home** icon as shown in the below image.



The **Pegasus™ Studio Home Screen** is displayed.



5 Ethernet

The **Ethernet** screen allows you to enable/disable and configure all the parameters related to the Ethernet interface available in Pegasus™ NX.

Configuration Instructions

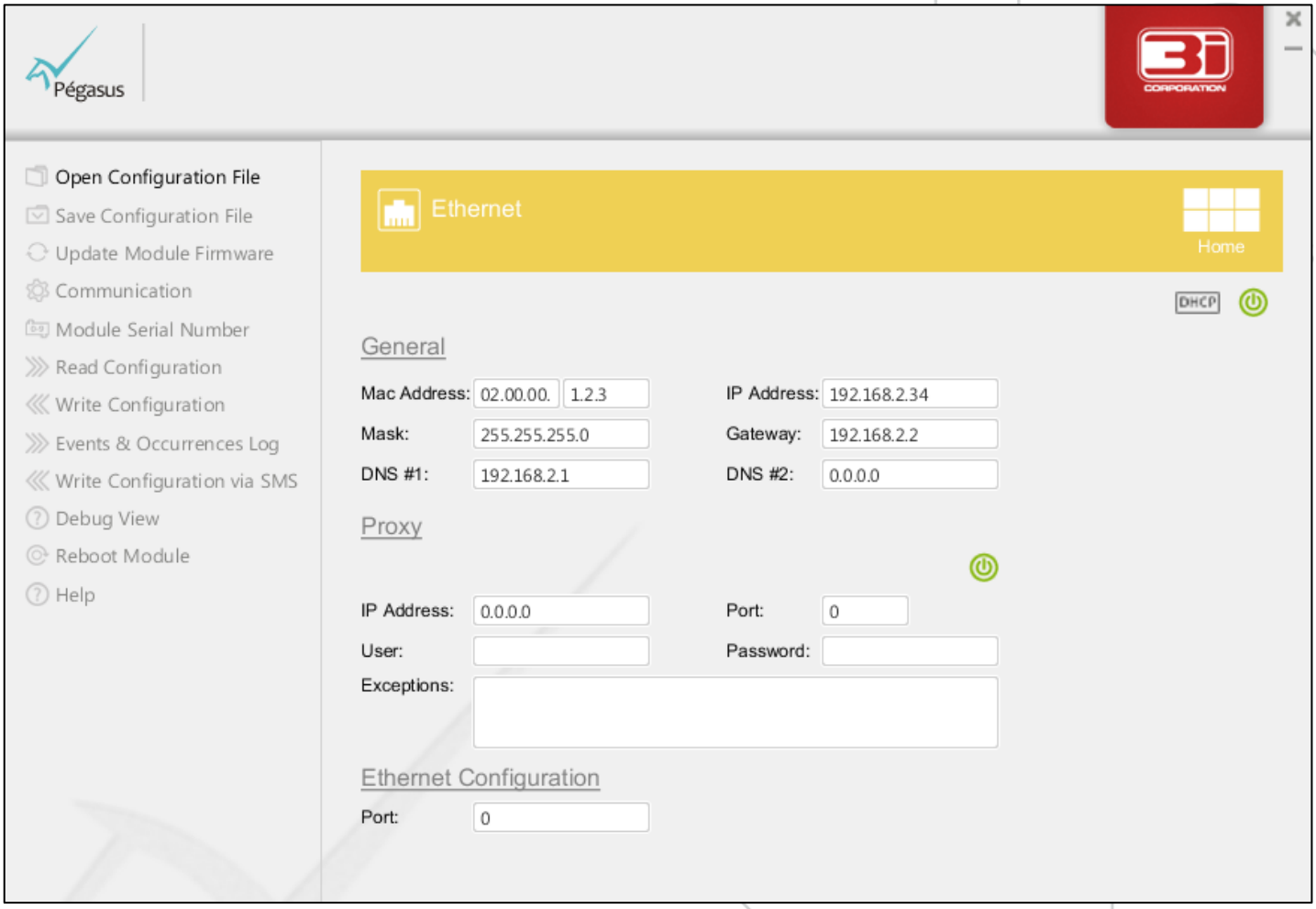
- To configure Ethernet, follow steps: 5.1 to 5.9.
- To configure Ethernet with DHCP enabled, skip step 5.3. Configure the General Ethernet Settings (DHCP Disabled)
- To configure Ethernet without Proxy, skip step 5.5. Enable the Proxy Interface, and step 5.6. Configure Proxy
- To write the Ethernet configuration to Pegasus™ NX, follow step 5.7. Write Configuration. To apply the Ethernet configuration settings, follow step 5.8. Reboot Module.

5.1. Open the Ethernet Screen

To open the ethernet screen

1. On the **Pegasus™ Studio Main Screen**, place your cursor on the **Ethernet** section, and then click to open the **Ethernet** screen.

The **Ethernet** screen is displayed as shown below.

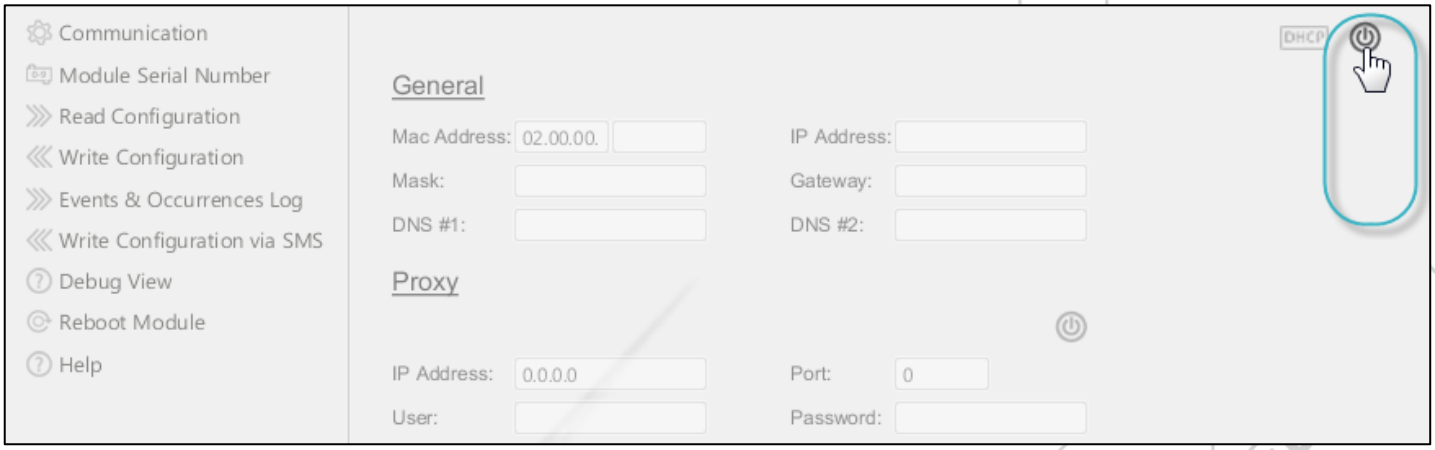


5.2. Enable the Ethernet Interface

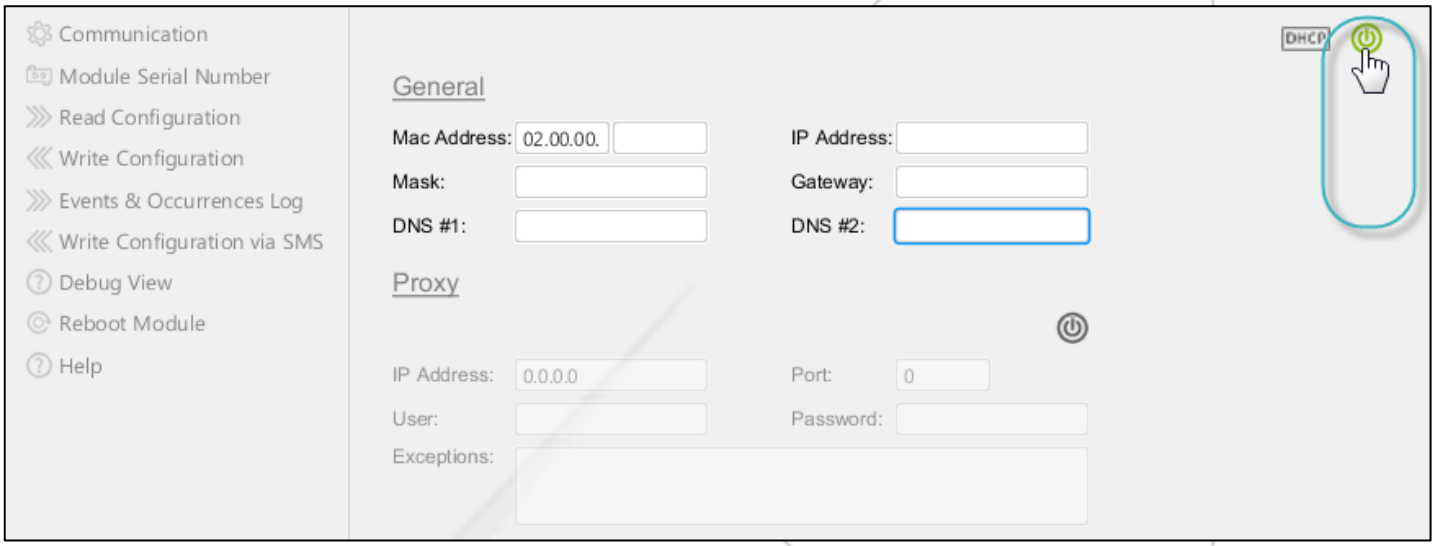
To configure the Etherent settings, it is required to enable the Ethernet interface. Until the Etherent interface is enabled, all the fields and options in the Ethernet screen are in the disabled state.

To enable the ethernet interface

1. Click the grey colored **Enable**  icon.



The grey colored icon is turned green  as shown in the below image. The Ethernet interface is in the enabled state.

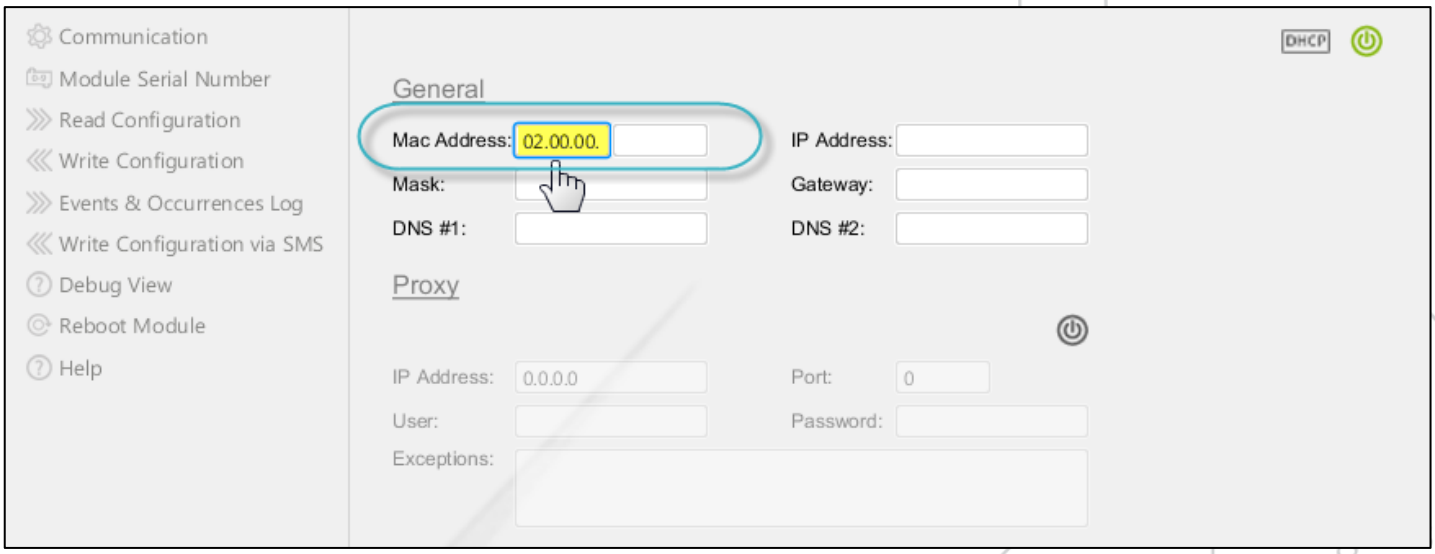


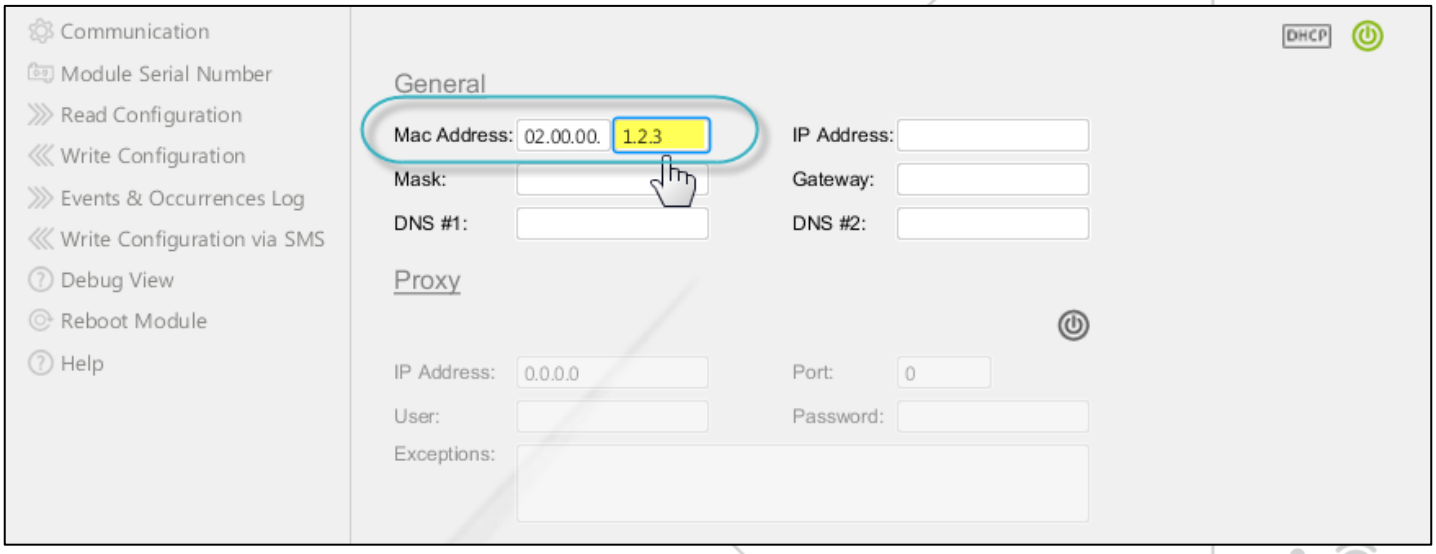
5.3. Configure the General Ethernet Settings (DHCP Disabled)

This section permits you to configure the general ethernet settings: Mac Address, IP Address, Mask, Gateway, DNS #1 and DNS#2.

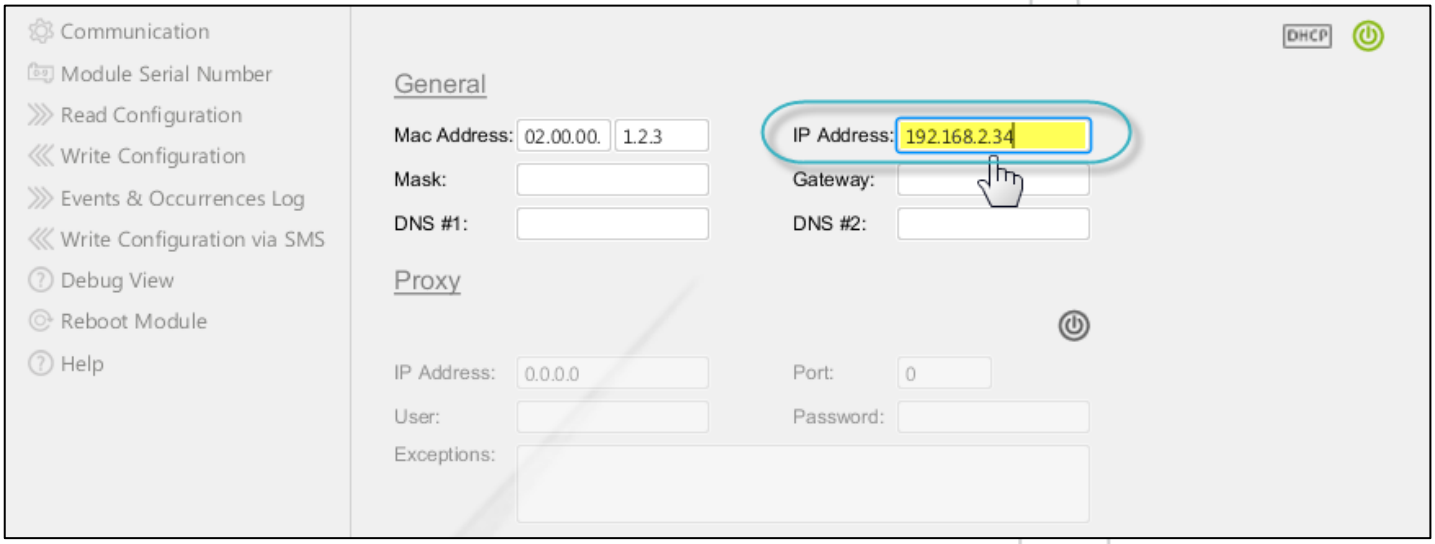
To configure the general ethernet settings

1. In the **Mac Address** text box, enter the **MAC Address**. The first field contains the predefined fixed values as shown in the below image. In the second field, type-in the remaining address.

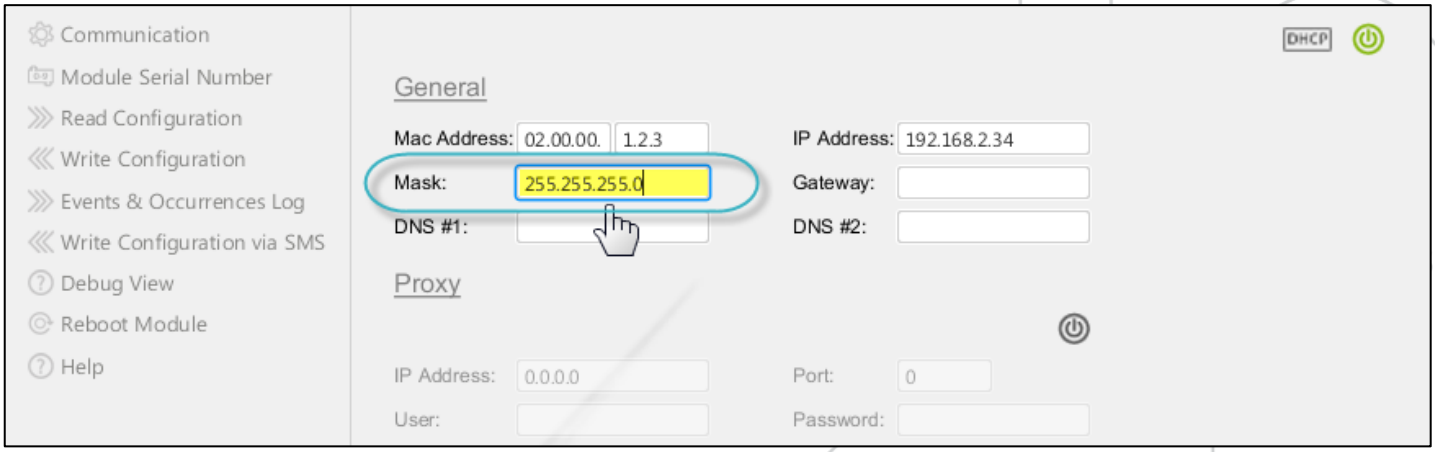




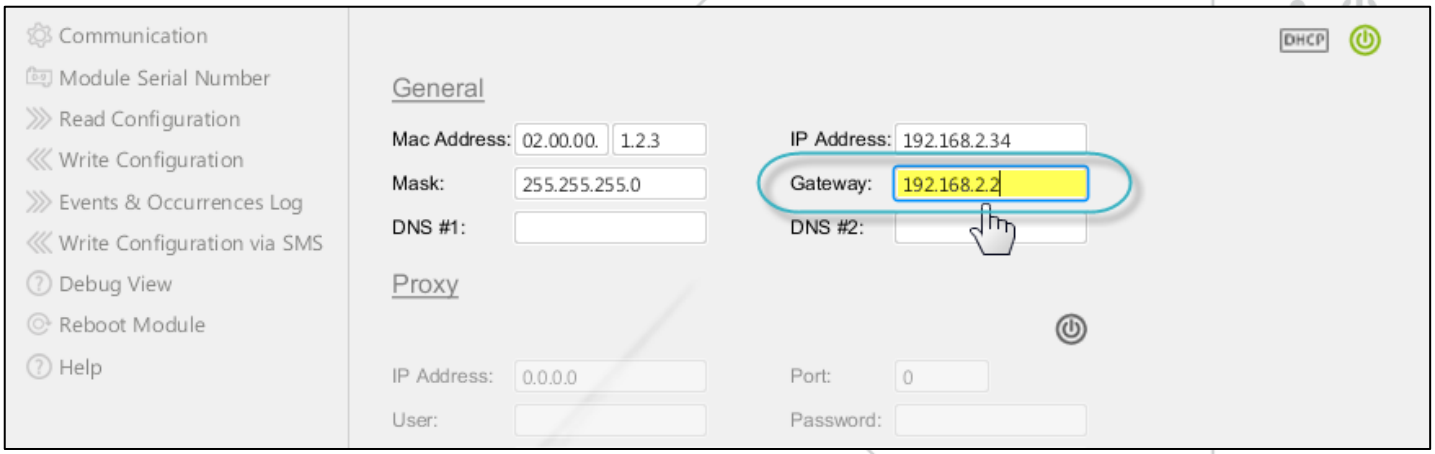
2. In the **IP Address** text box, enter the **Internet Protocol Address**.



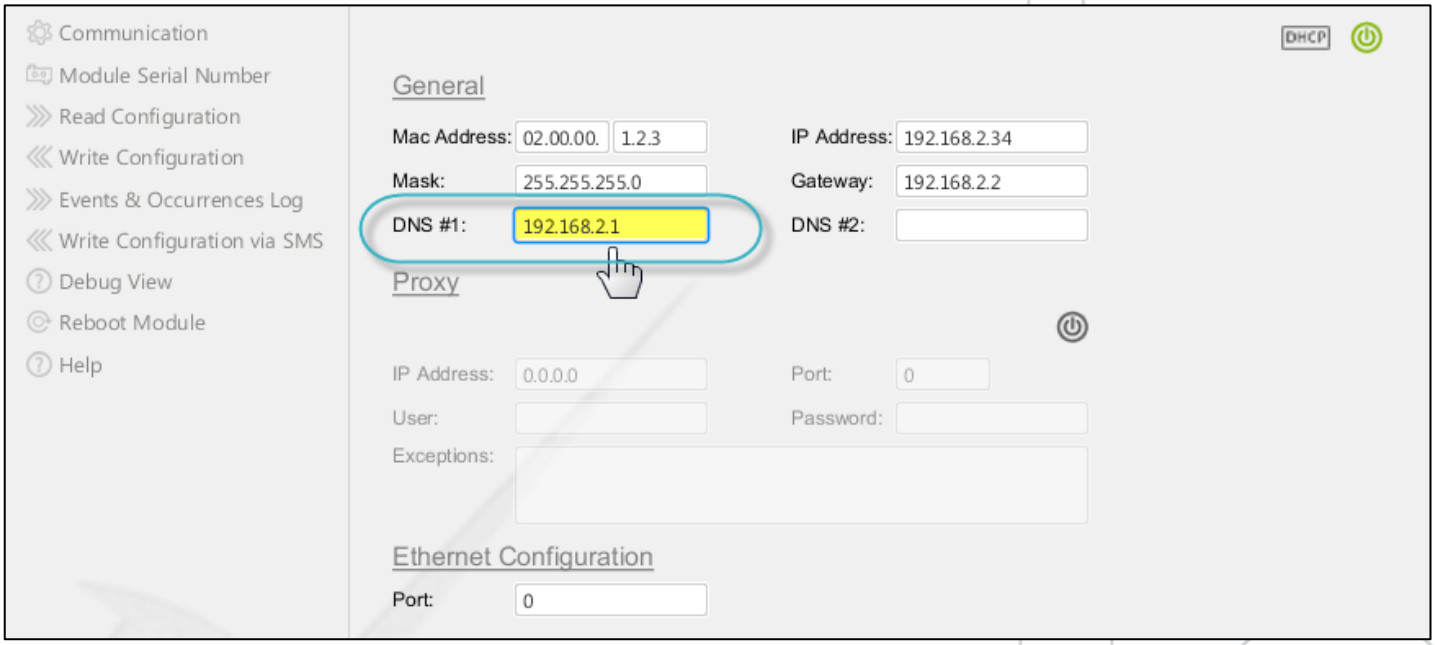
3. In the **Mask** text box, enter the **Subnet Mask** to mask the IP Address (to divide IP address into network address and host address)**.**



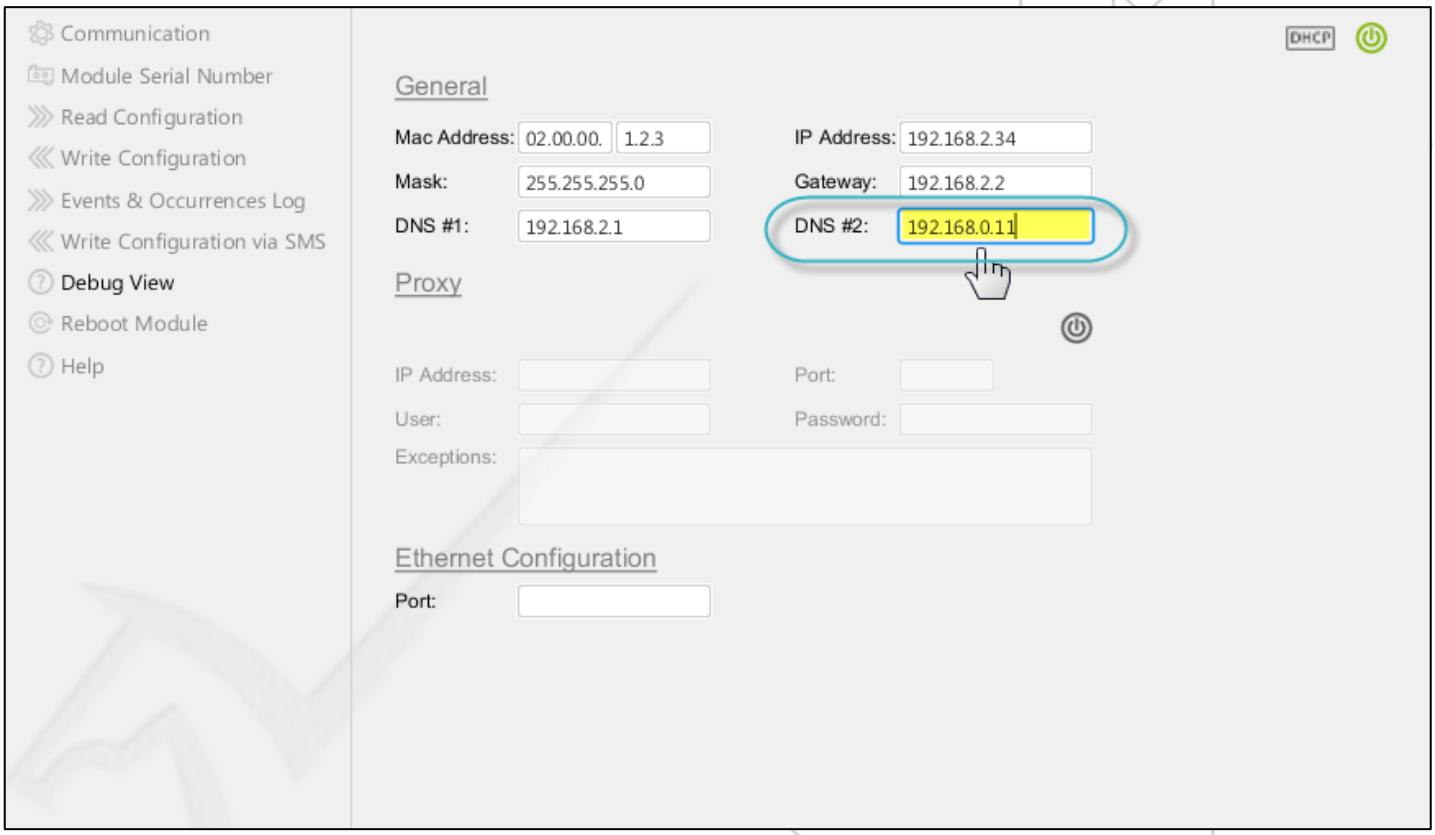
4. In the **Gateway** text box, enter the **Gateway Address** (a network node equipped for interfacing with another network that uses different protocols).



5. In the **DNS #1** text box, enter the first **Domain Name Service**.



6. In the **DNS #2** field, enter the second **Domain Name Service**.



5.4. Configure the General Ethernet Settings (DHCP Enabled)

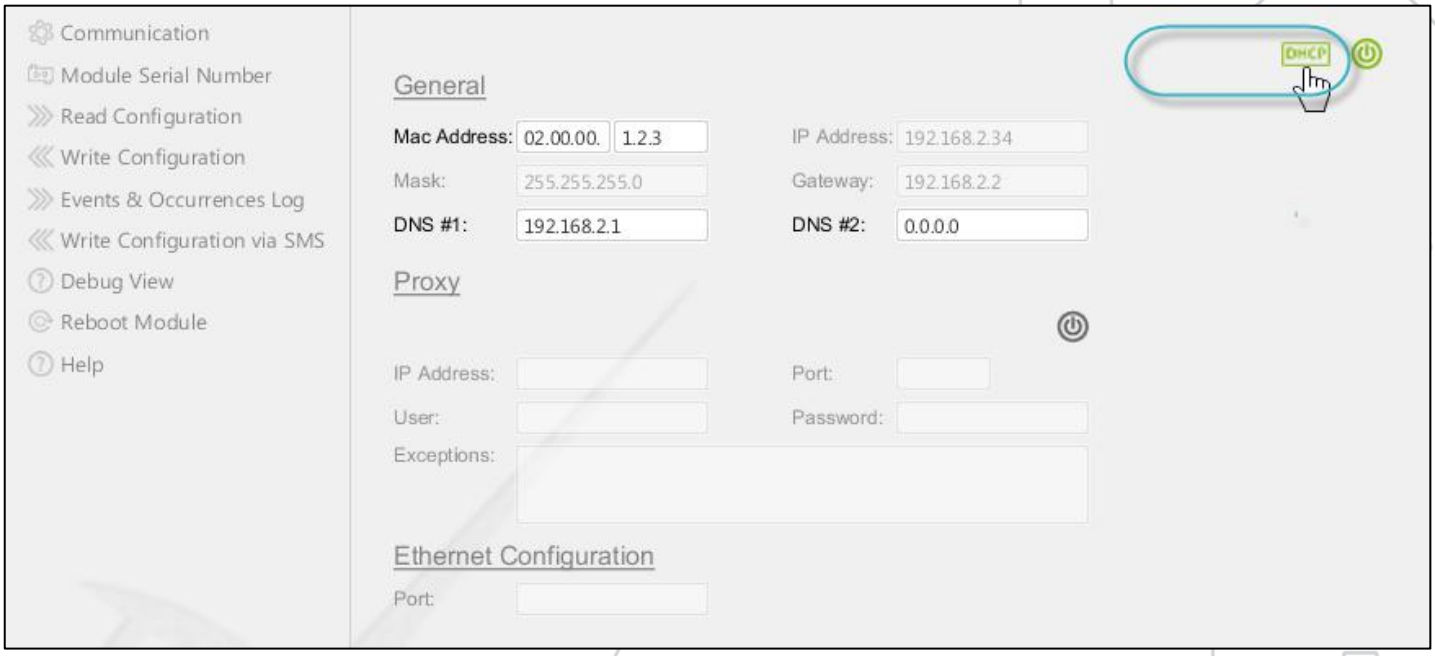
DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, Pegasus™ NX can have a different IP address every time it connects to the network.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task.

5.4.1. Enable DHCP

To enable DHCP

1. Click the grey colored **DHCP**  icon. The grey colored icon is turned green  as shown in the below image. DHCP is in the enabled state.



5.4.2. Configure the General Ethernet Settings

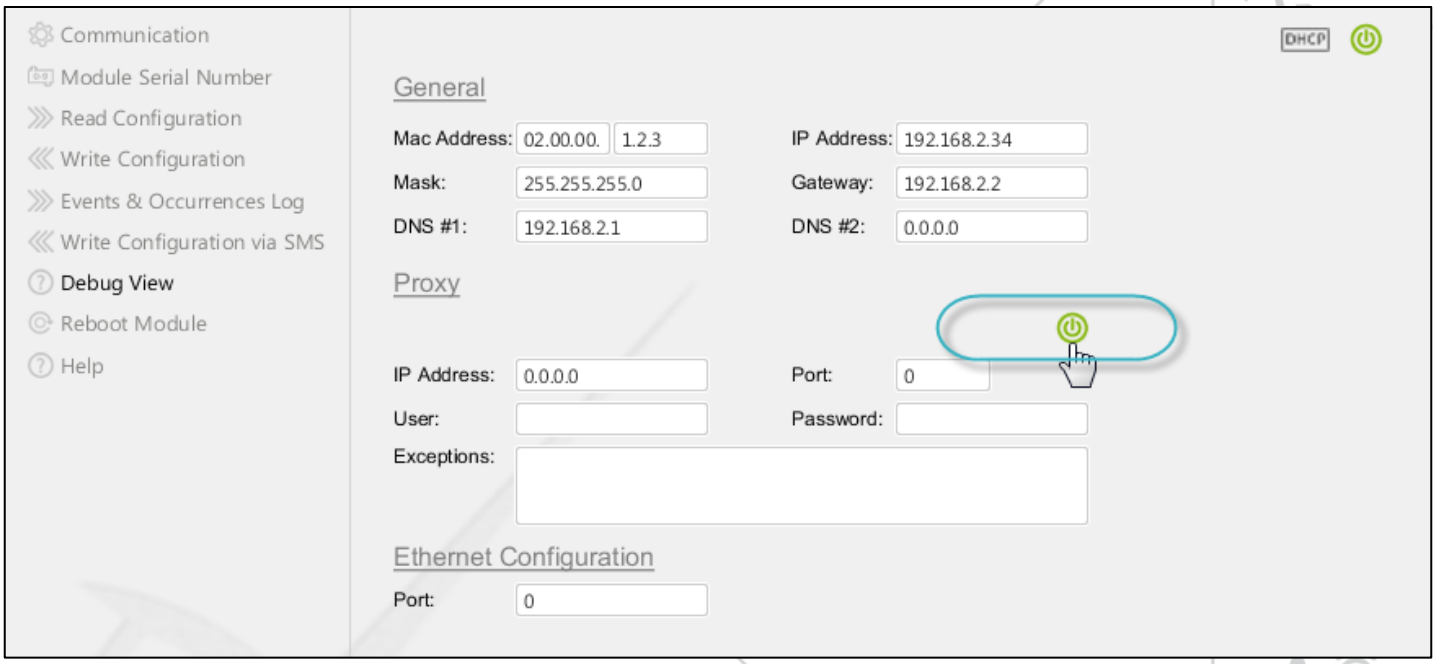
You can configure the General Ethernet settings exactly as per the instructions provided in Step 5.3. In DHCP enabled condition, only the IP Address, Mask and Gateway fields are disabled.

5.5. Enable the Proxy Interface

To enable the proxy interface

1. Click the grey colored **Use Proxy Server**  icon.

The grey colored icon is turned green  as shown in the below image. The Proxy interface is in the enabled state.



You can configure the Proxy settings as per the instructions provided in Step 6: Configure Proxy.

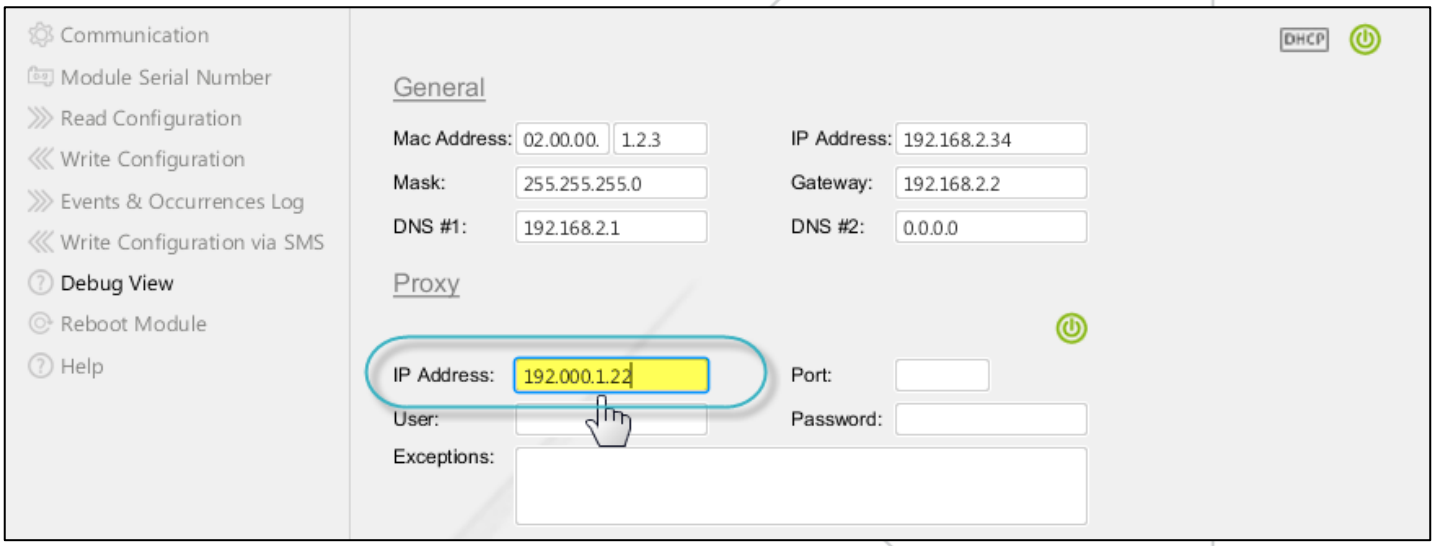
5.6. Configure Proxy

Pegasus™ Studio allows you to configure proxy. In computer networks, a proxy module acts as an intermediary for requests from clients seeking resources from other modules. A client connects to the proxy module, requesting some service, such as a file, connection, web page, or other resource available from a different module. The proxy module evaluates the request as a way to simplify and control their complexity. A proxy module has a variety of potential purposes, including:

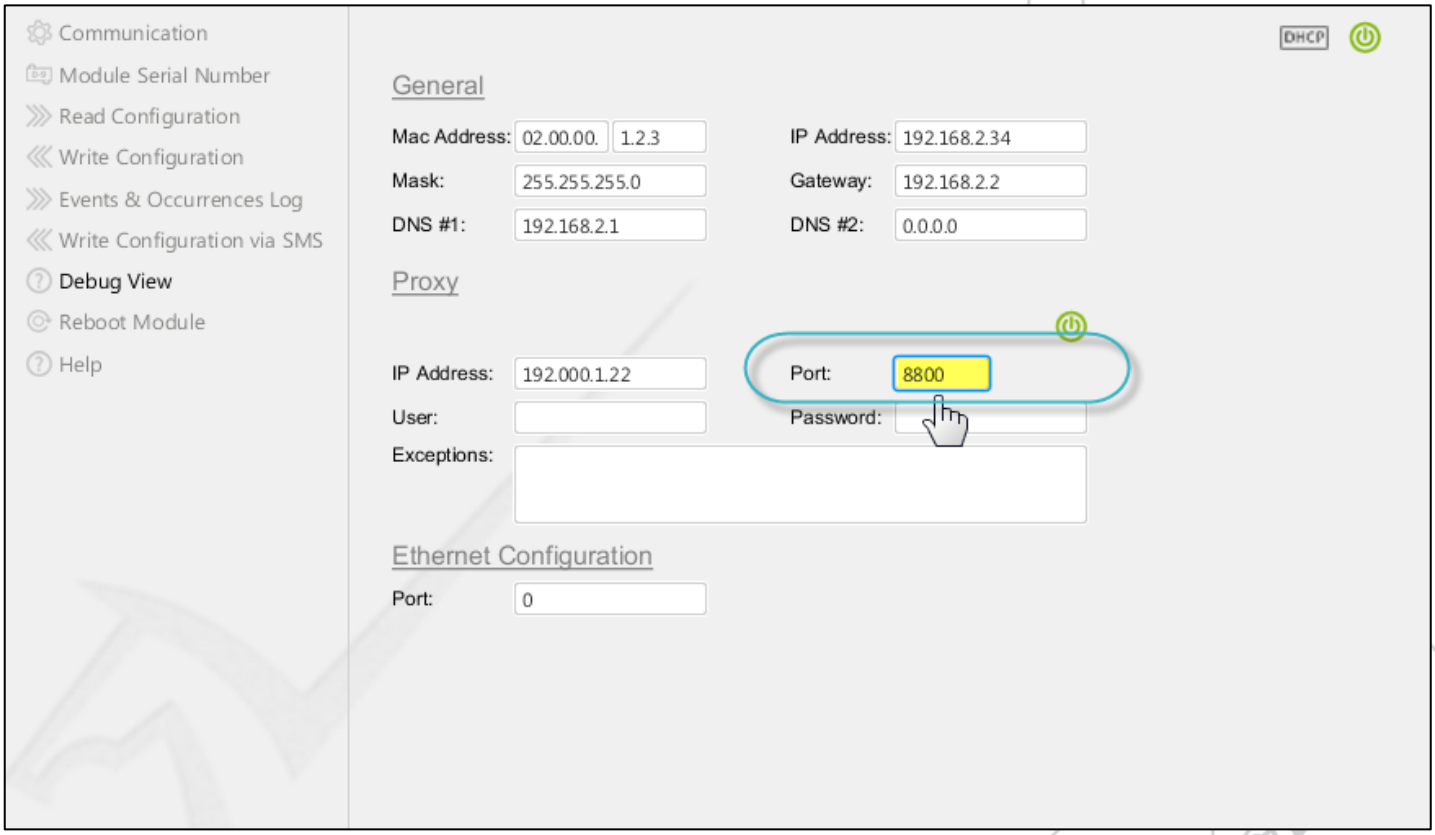
○ To keep machines behind it anonymous, mainly for security.	○ To speed up access to resources using caching.
○ To prevent downloading the same content multiple times, and thus saves bandwidth.	○ To scan outbound content, e.g., for data loss prevention.
○ To scan transmitted content for malware before delivery.	○ Access enhancement/restriction.

To configure proxy

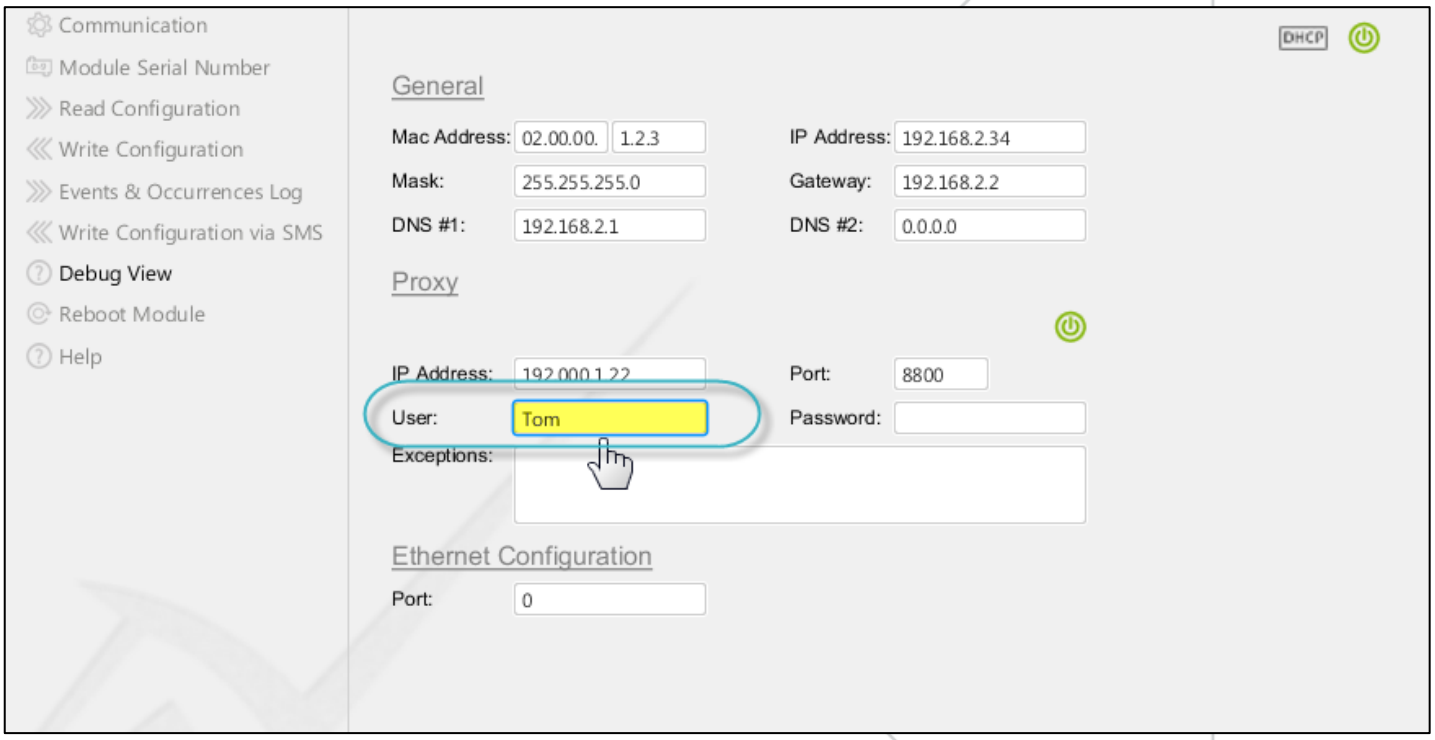
1. In the **IP Address** text box, enter the **IP Address** of the proxy server.



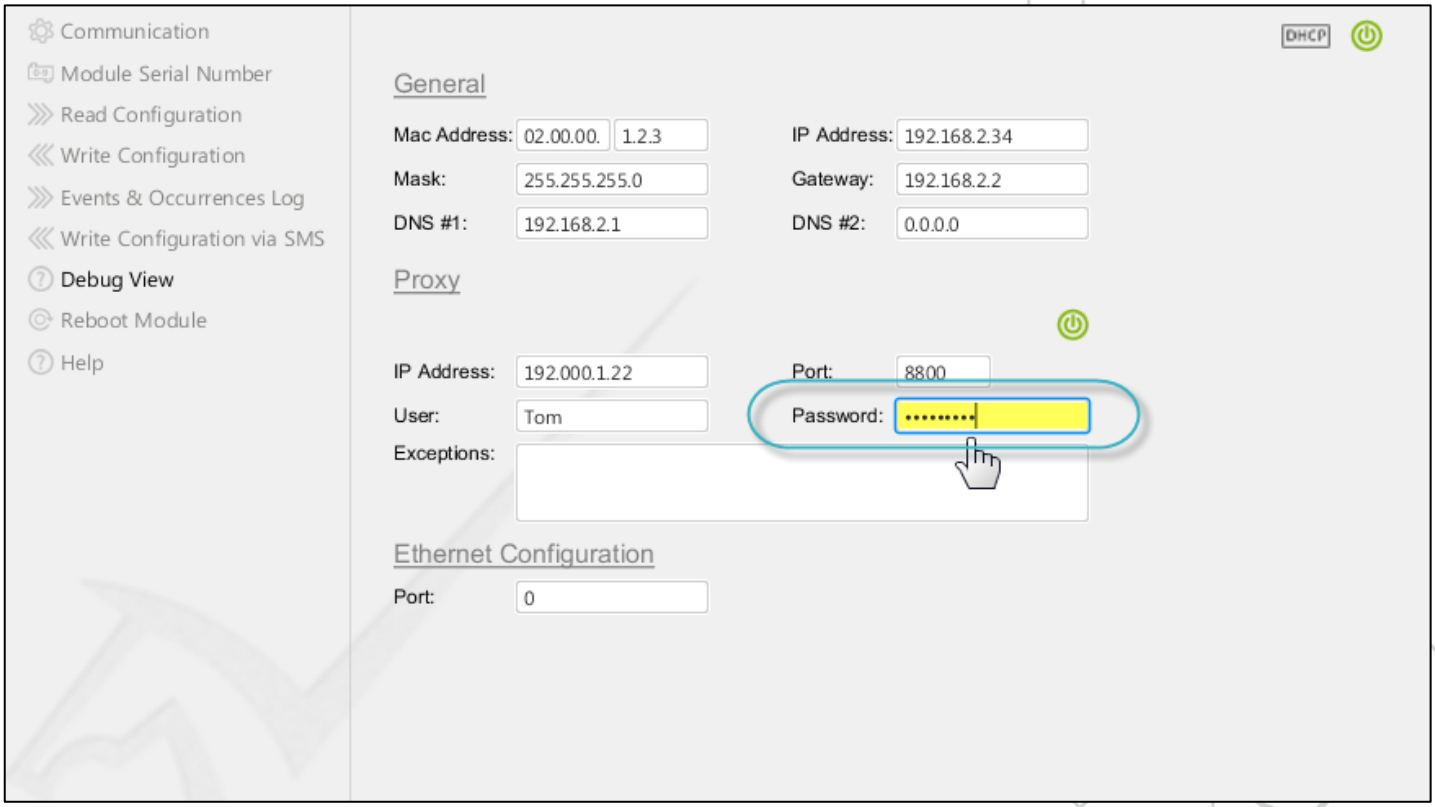
2. In the **Port** text box, enter the appropriate **Port** number.



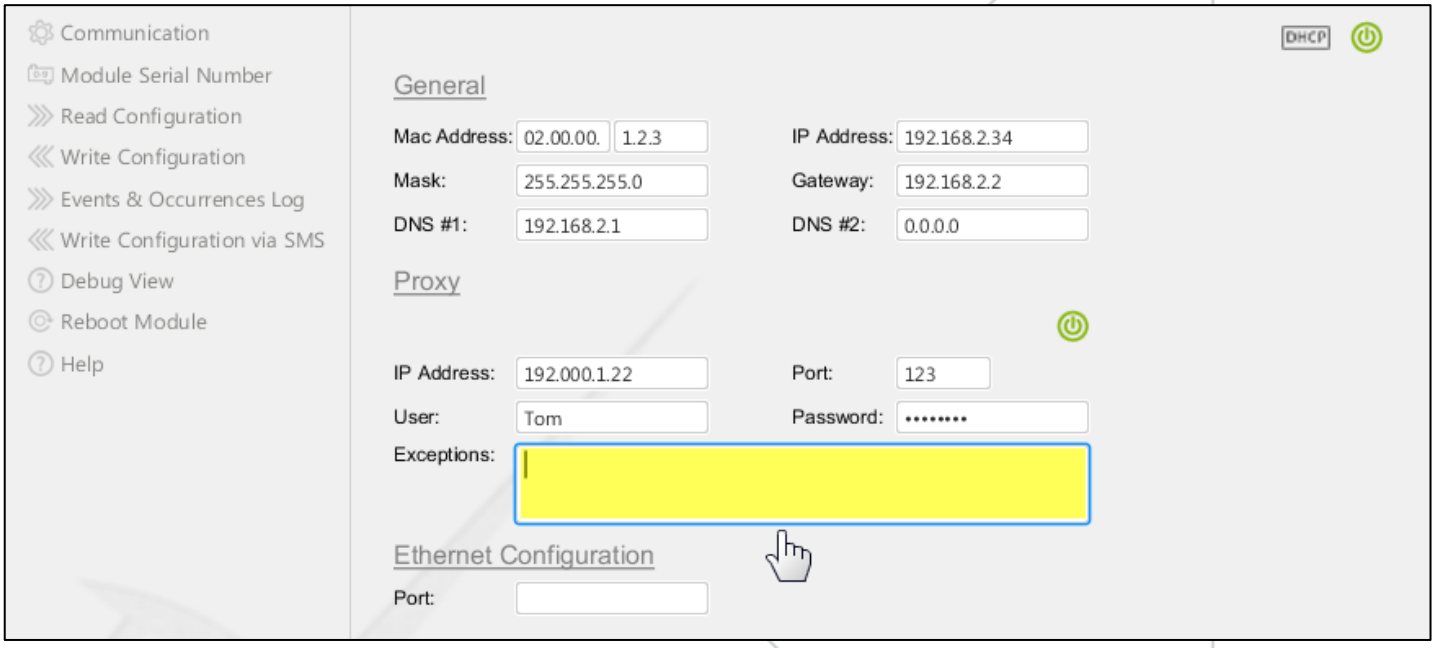
3. In the **User** text box, enter your **Username**.



4. In the **Password** text box, enter your **Password**.

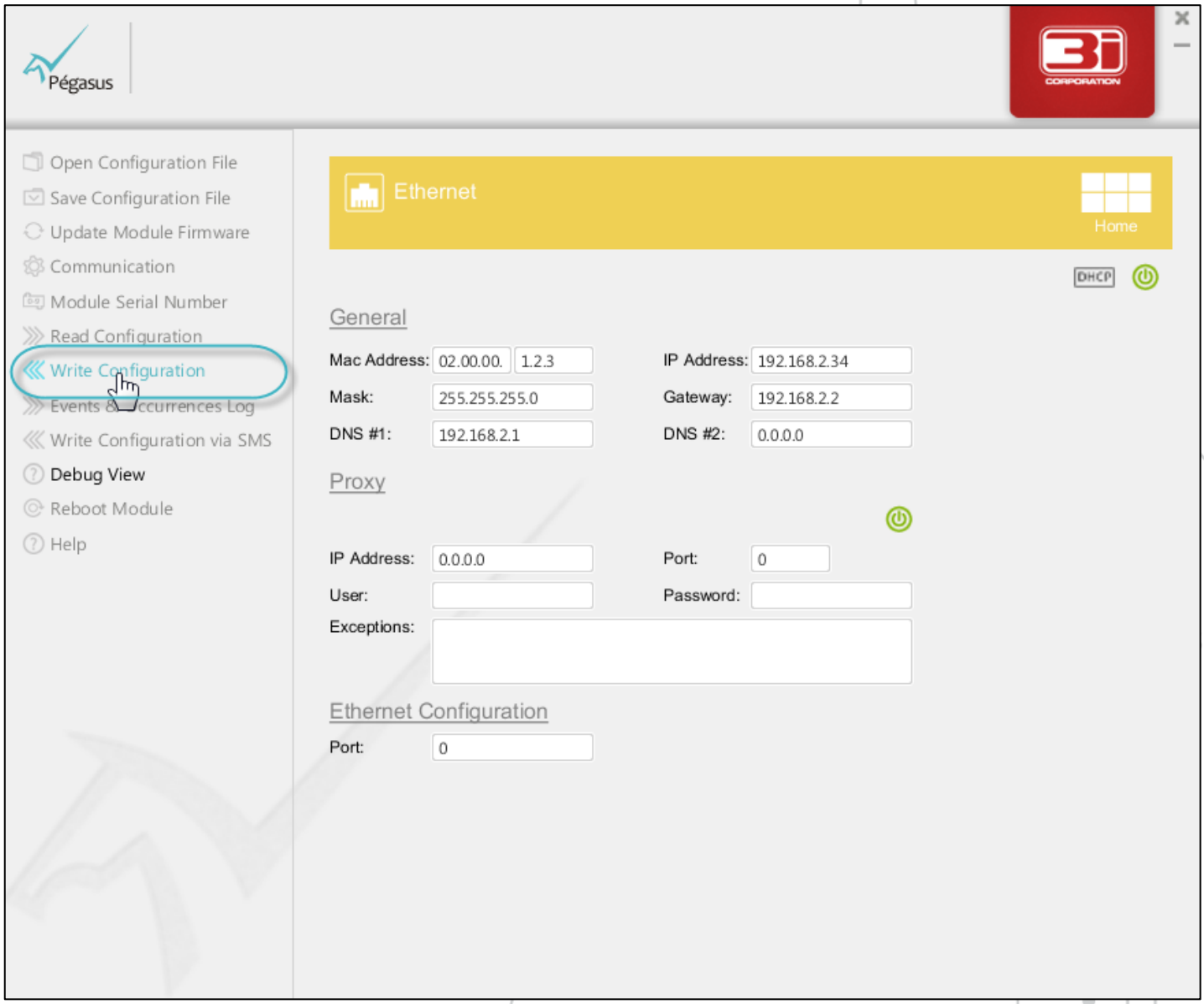


5. Under **Exceptions**, enter **Proxy Exceptions** separated by semi-colon.



5.7. Write Configuration

When the Ethernet configuration settings are done, write the configuration to Pegasus™ NX.

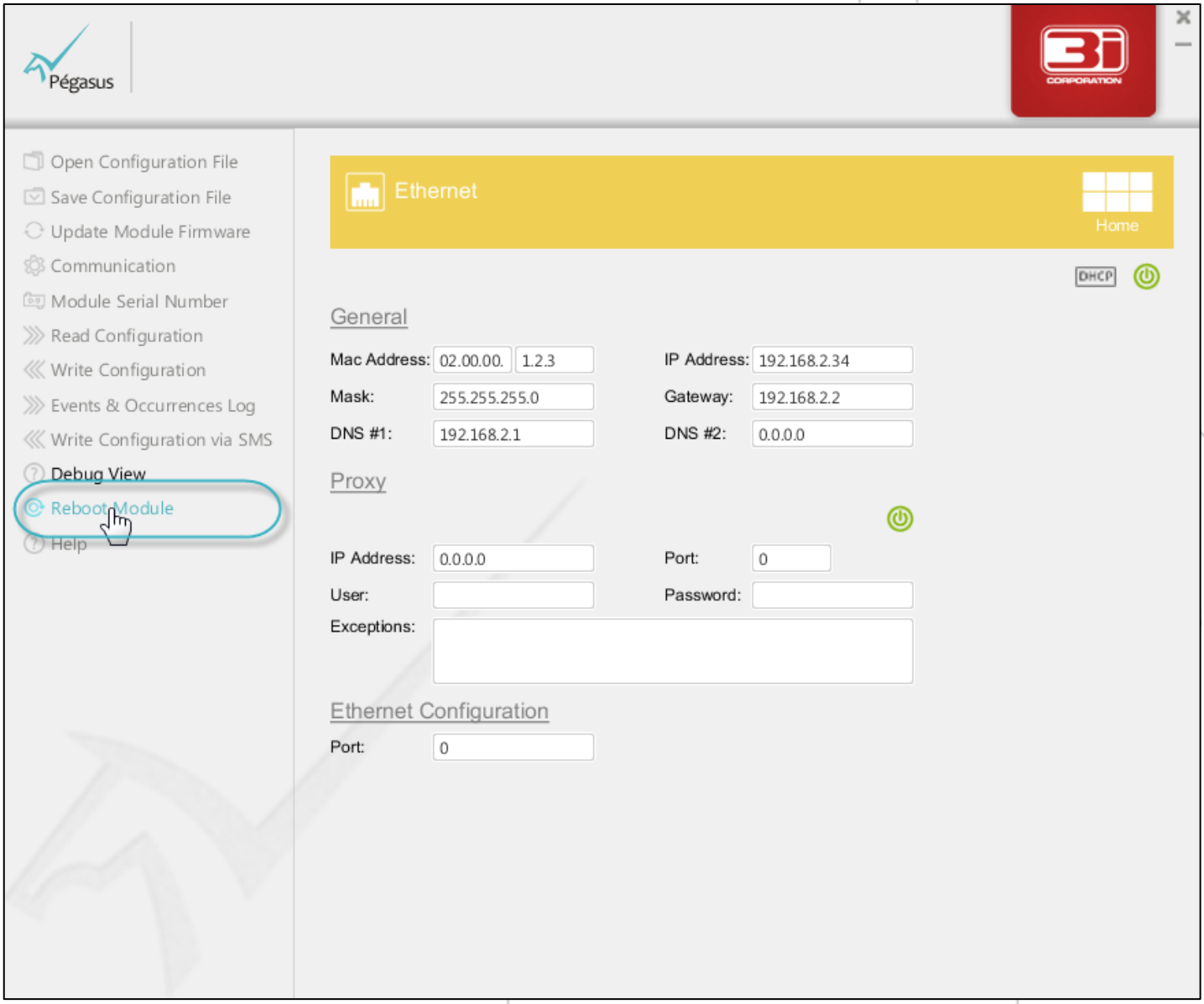


Note:

To learn how to write the configuration settings to Pegasus™ NX, refer the **Write Configuration** chapter.

5.8. Reboot Module

On successful writing of the Pegasus NX configfuration settings, to make all configured features functional, reboot of module is required.



Note:

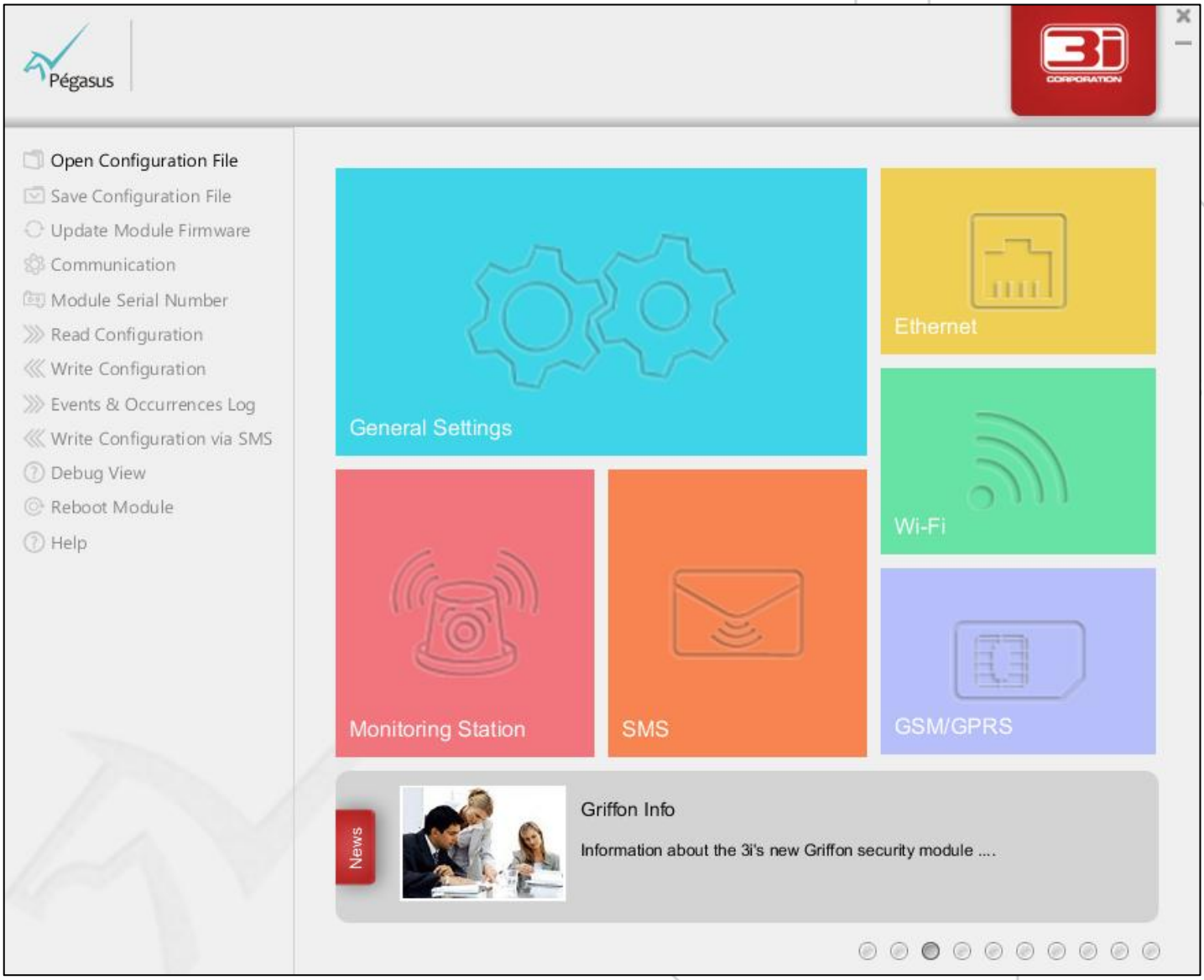
To learn how to reboot module after writing the configuration to Pegasus™ NX, refer the **Reboot Module** chapter.

5.9. Return Back to Home Screen

To return back to the home screen

2. Click the **Home** icon as shown in the below image.

The **Pegasus™ Studio Home Screen** is displayed.



6 Wi-Fi

The **Wi-Fi** screen allows you to enable/disable, and configure all the parameters related to the Wi-Fi interface available in Pegasus™ NX.

Configuration Instructions

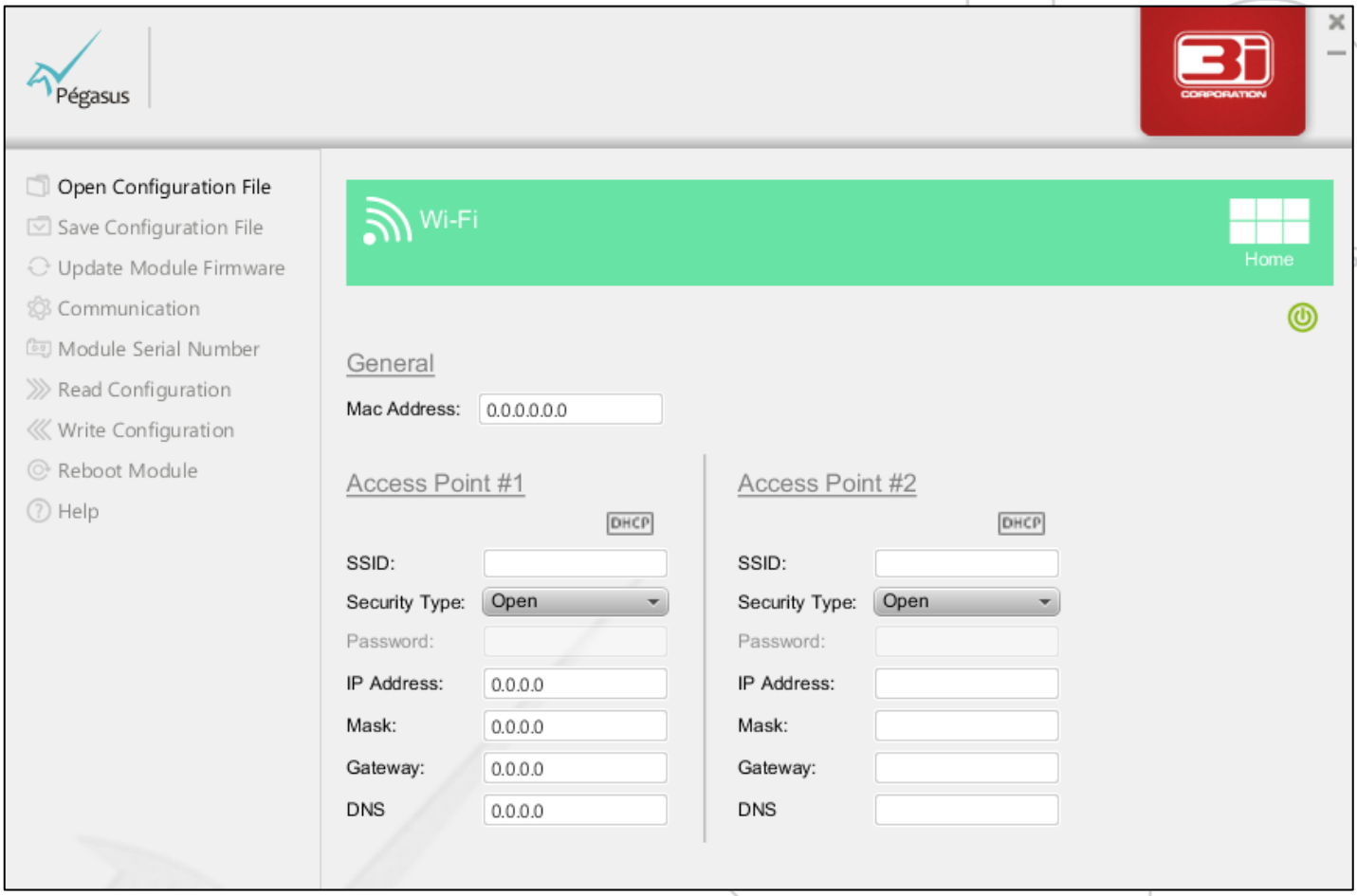
- To configure Wi-Fi, follow steps: 6.1 to 6.8.
- To configure Wi-Fi Access Points with DHCP enabled, skip step 6.3. Configure Access Points (DHCP Disabled)
- To write the Wi-Fi configuration to Pegasus NX, follow step 6.6. Write Configuration. To apply the Wi-Fi configuration settings, follow step 6.7. Reboot Module.

6.1. Open the Wi-Fi Screen

To open the wi-fi screen

1. On the **Pegasus™ Studio Main Screen**, place your cursor on the **Wi-Fi** section, and then click to open the **Wi-Fi** screen**.**

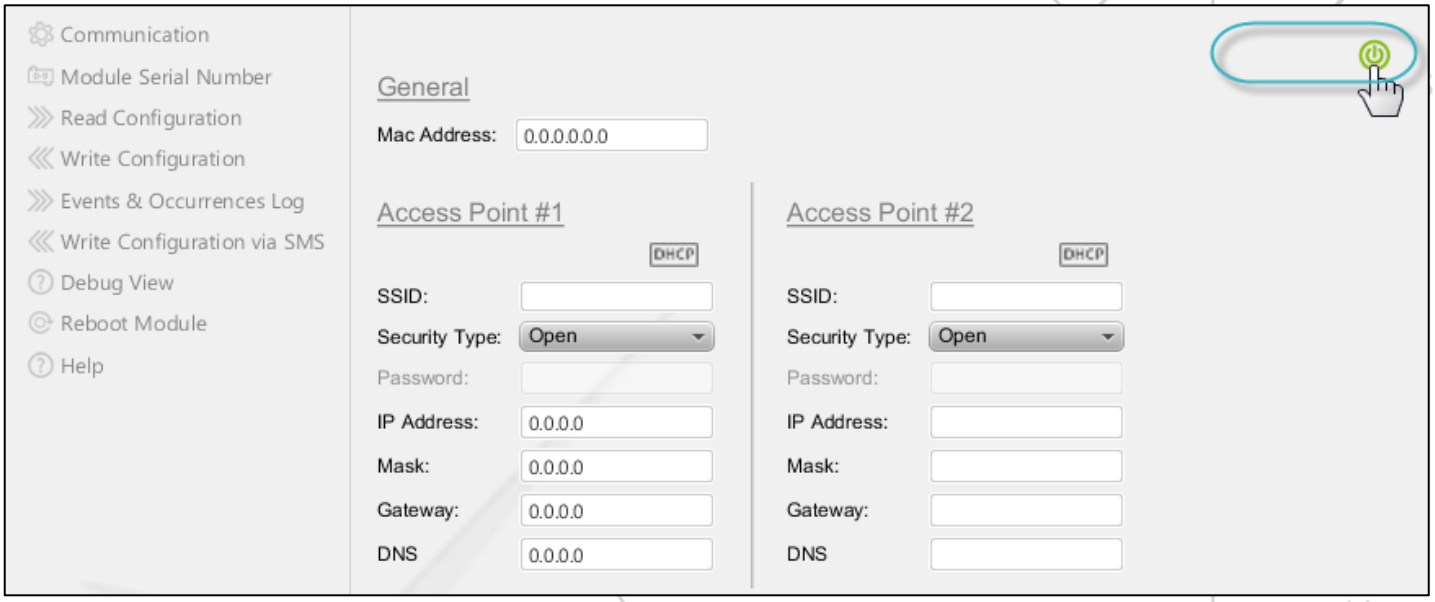
The **Wi-Fi** screen is displayed as shown below.



6.2. Enable the Wi-Fi Interface

To enable the wi-fi interface

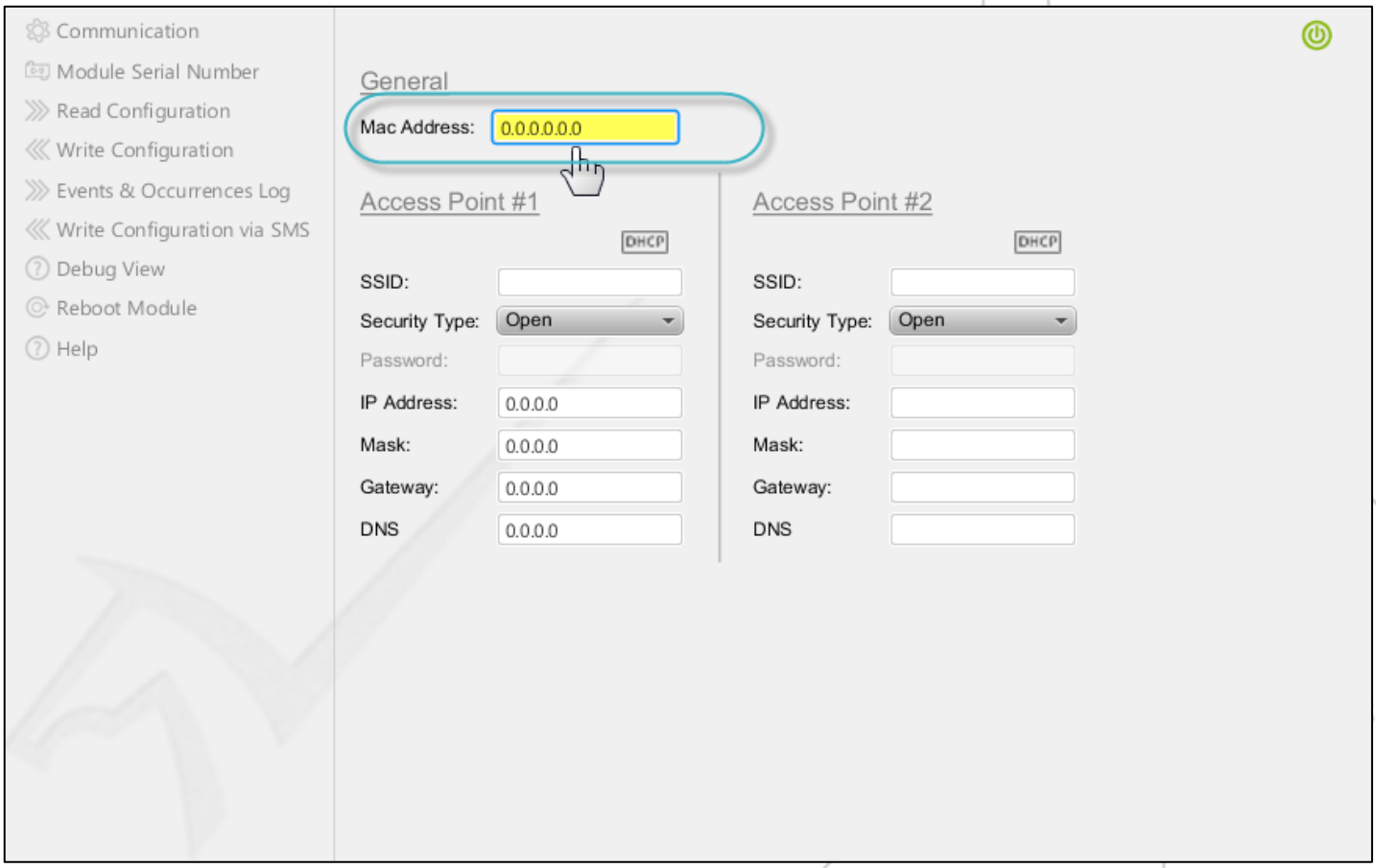
1. Click the grey colored **Enable**  icon.



6.3. Configure the General Wi-Fi Settings

To configure the general wi-fi settings

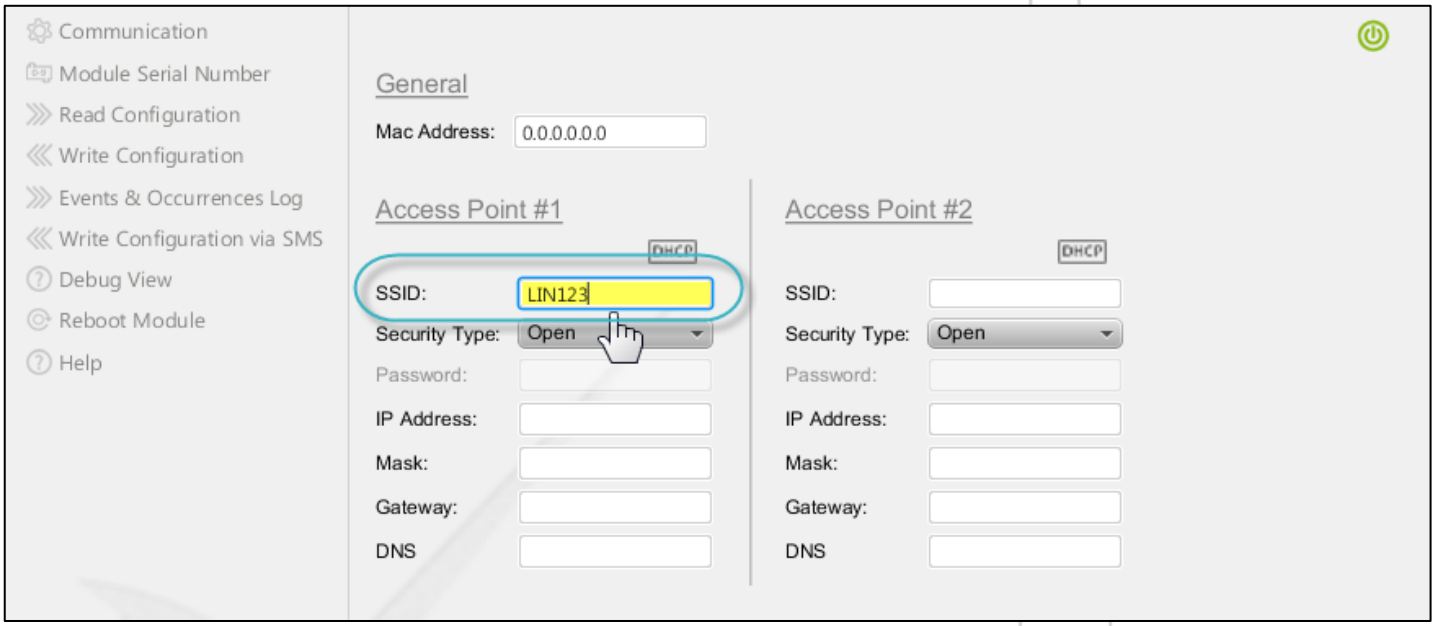
1. In the **Mac Address** text box, enter the **Media Access Control** Address.



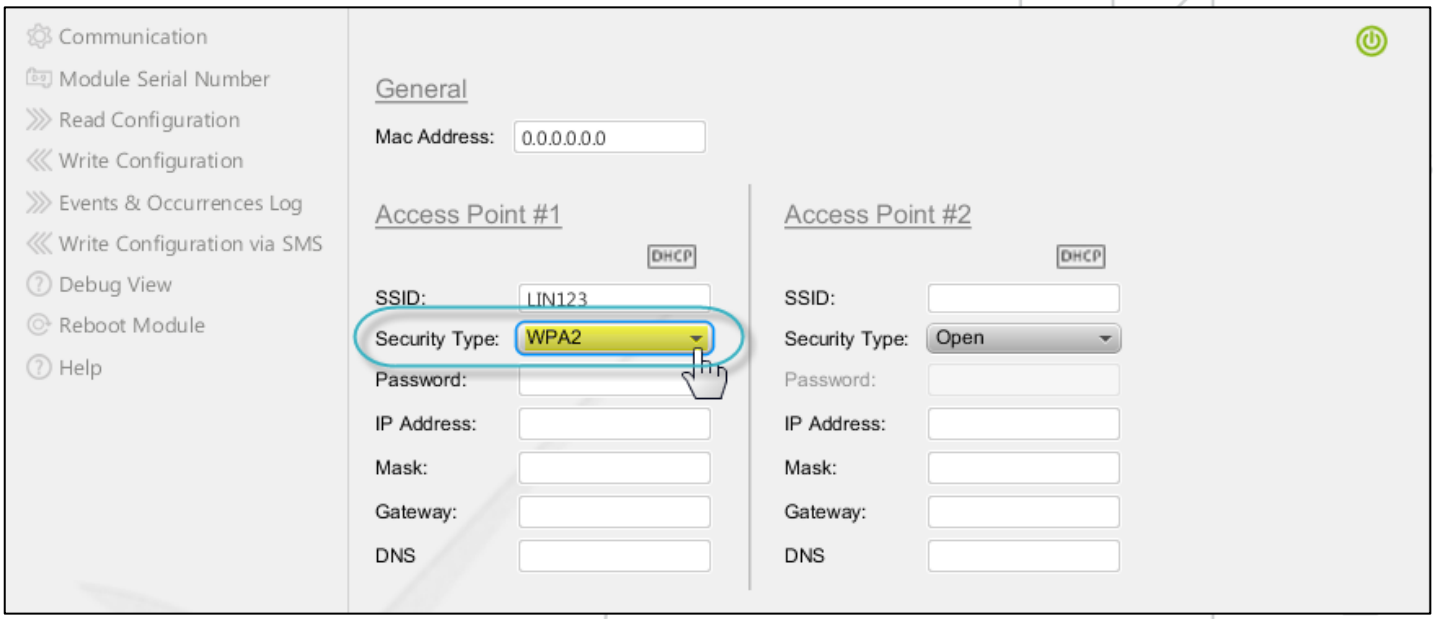
6.4. Configure Access Points (DHCP Disabled)

To configure access points

1. Under Access Point #1, in the **SSID** text box, enter **Service Set Identifier.** This is the name your wireless access point will broadcast. For example, the default SSID for a Linksys router is Linksys. It is recommended that you change the SSID to something you recognize.



2. In the **Security Type** drop-down box, select the type of encryption you want. You can choose: **Open**, **WEP WPA**, or **WPA2**.

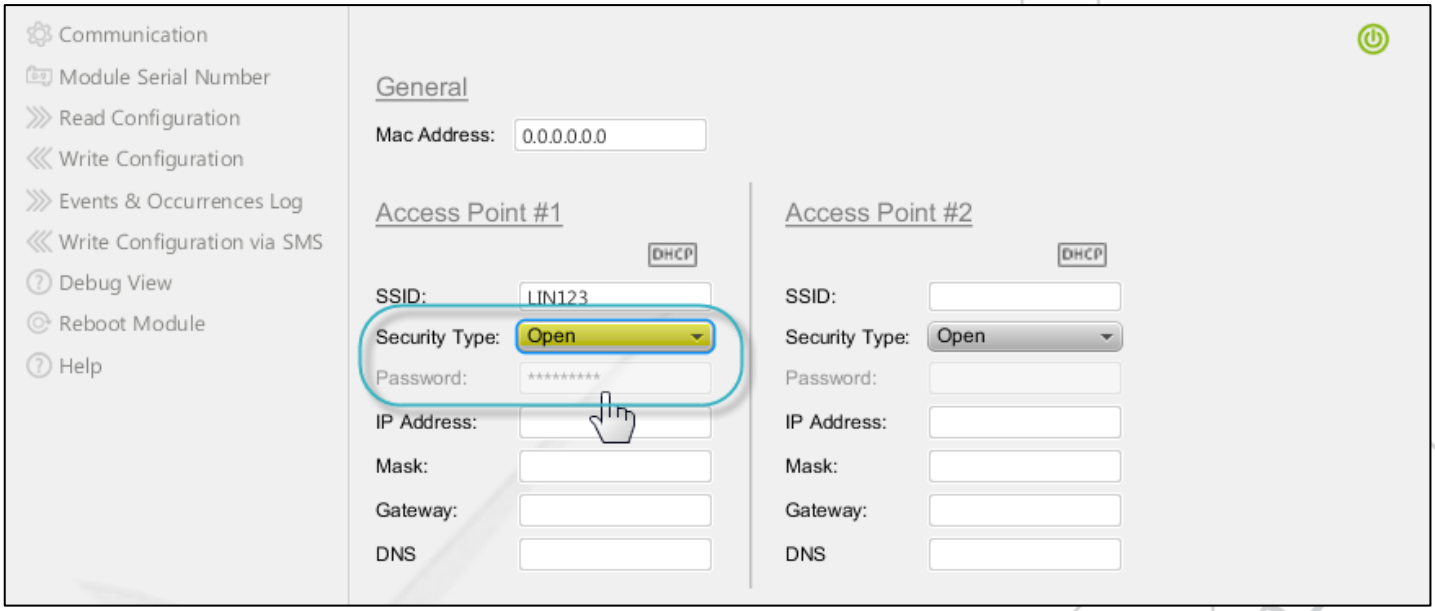


Warning:

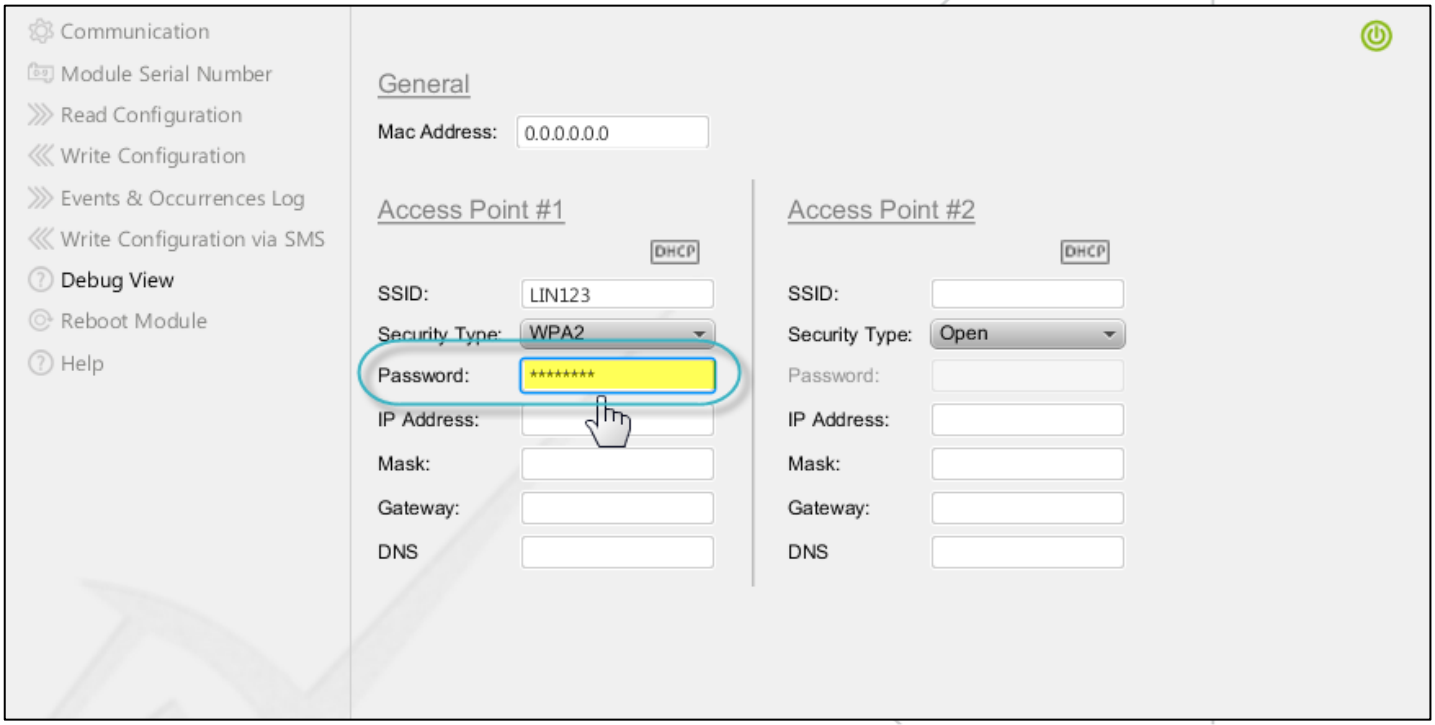
If you select the security type as **Open**, the Wi-Fi network might allow unauthorized access and will not be secured.

Note:

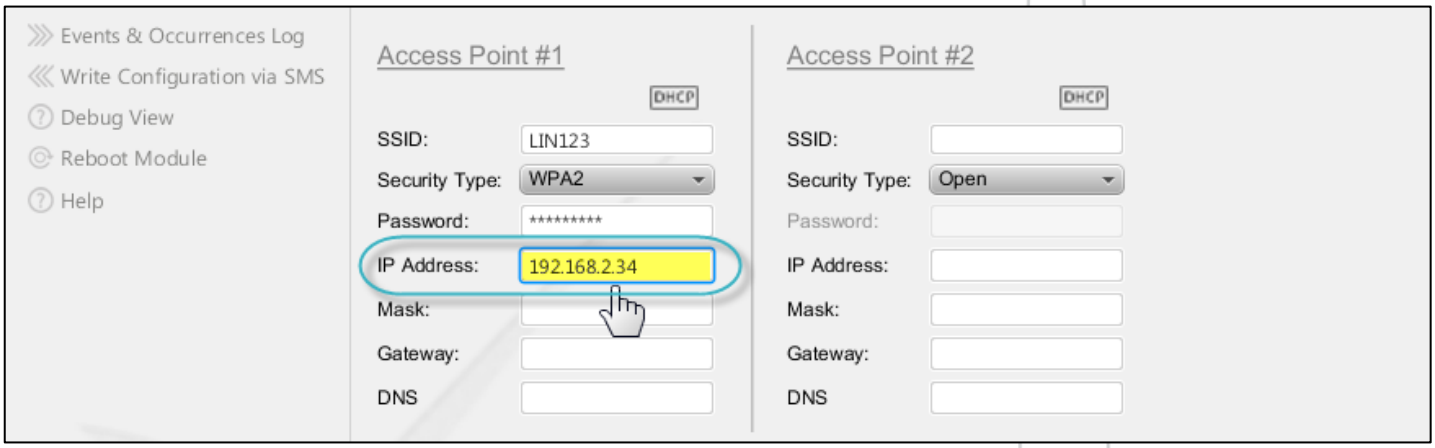
If you select the Security Type as **Open**, then the password setup is not required and the **Password** text box will be in the disabled mode.



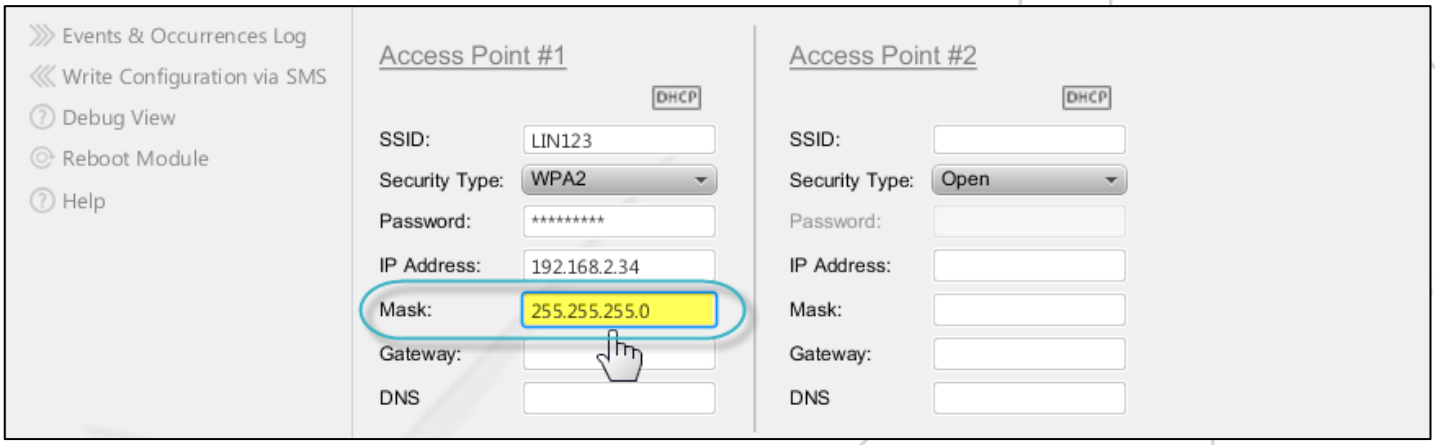
3. In the **Password** text box, enter your **Password**. It is recommended to assign a strong password for security purposes.



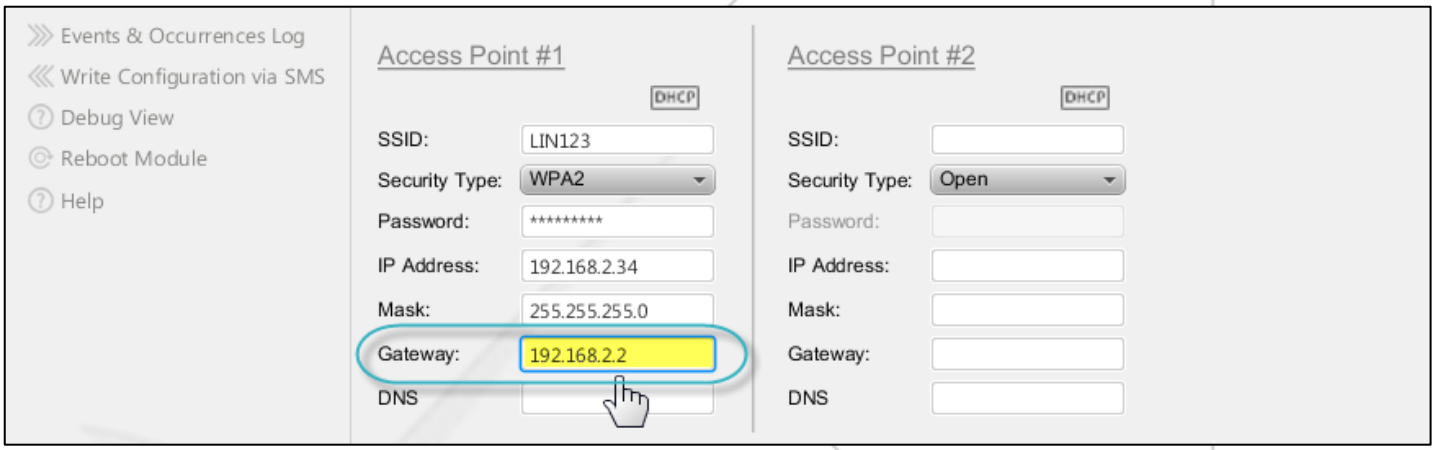
4. In the **IP Address** text box, enter the **Internet Protocol Address.**



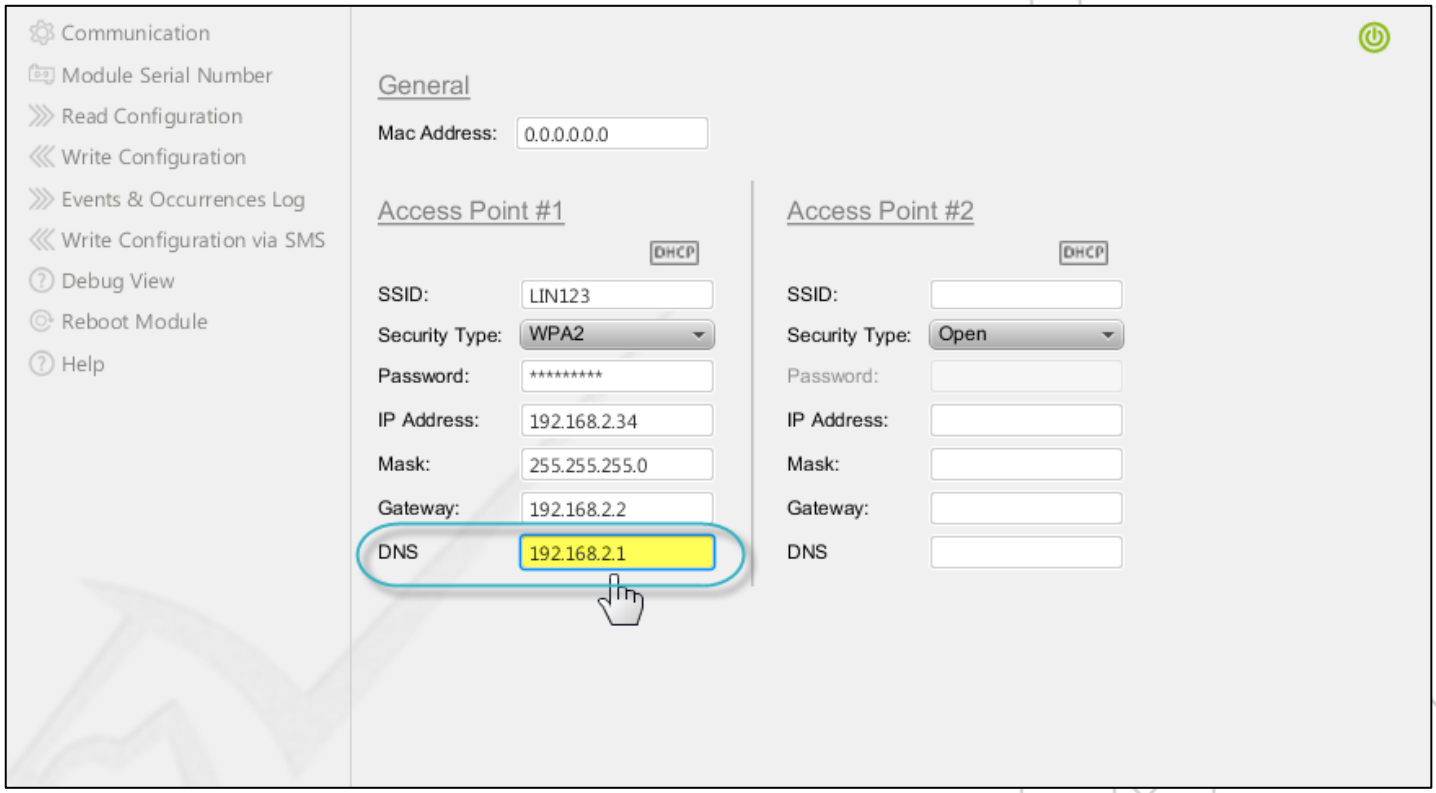
5. In the **Mask** text box, enter the **Subnet Mask** to mask the IP Address (to divide IP address into network address and host address)**.**



6. In the **Gateway** text box, enter the **Gateway Address** (a network node equipped for interfacing with another network that uses different protocols).



7. In the **DNS** text box, enter **Domain Name Service**.



8. Likewise, you can configure **Access Point #2** settings.

6.5. Configure Access Points (DHCP Enabled)

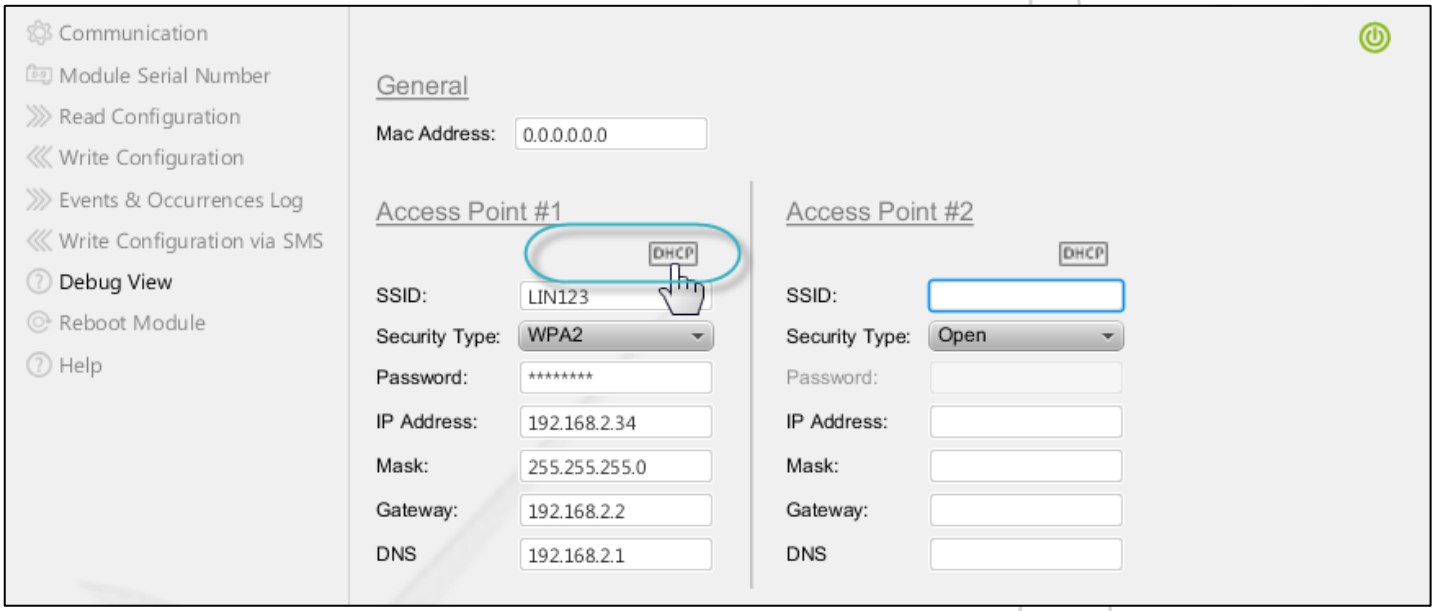
DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, Pegasus™ NX can have a different IP address every time it connects to the network.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task.

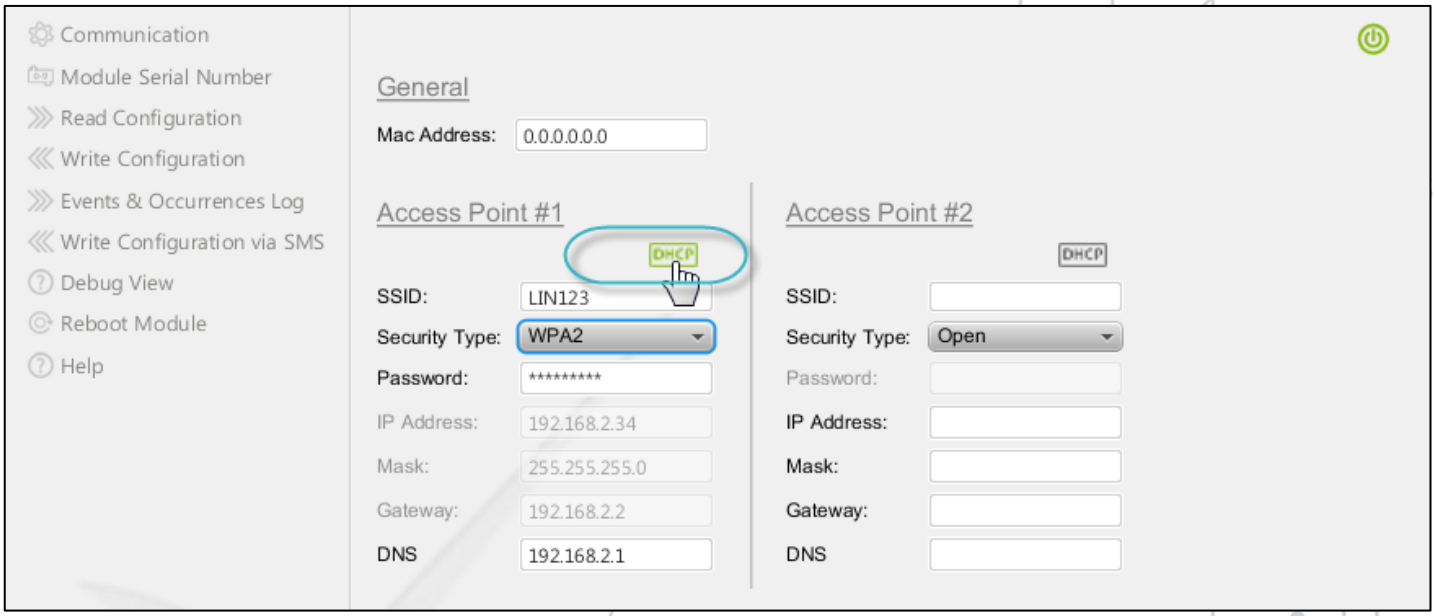
6.5.1. Enable DHCP

To enable DHCP

1. Click the grey colored **Use DHCP**  icon.



2. The grey colored icon is turned green  as shown in the below image. DHCP is in the enabled state.

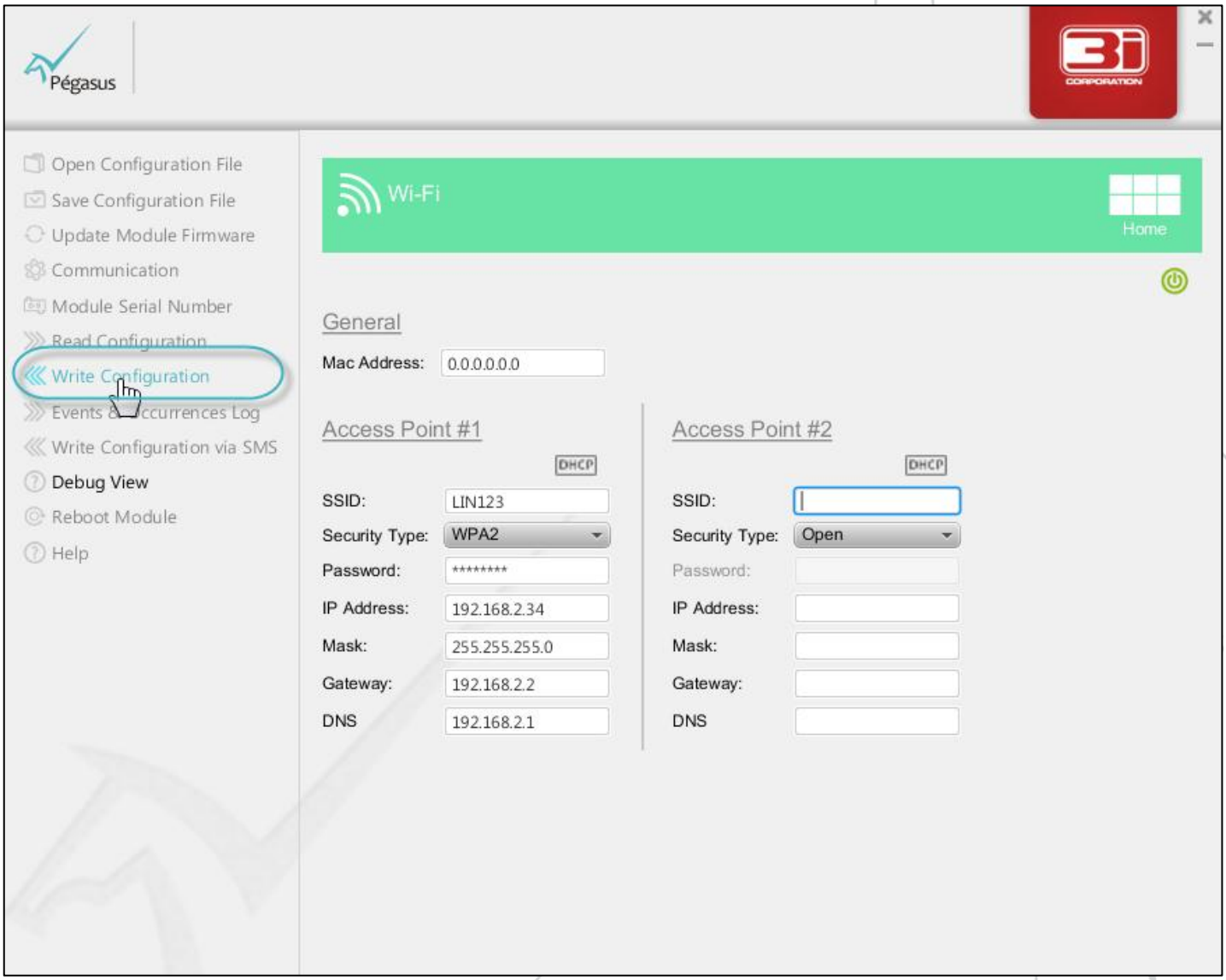


6.5.2. Configure Access Points

You can configure the Access Point settings exactly as per the instructions provided in Step 4. In DHCP enabled condition, only the IP Address, Mask and Gateway fields are disabled.

6.6. Write Configuration

When the Wi-Fi configuration settings are done, write the configuration to Pegasus™ NX.

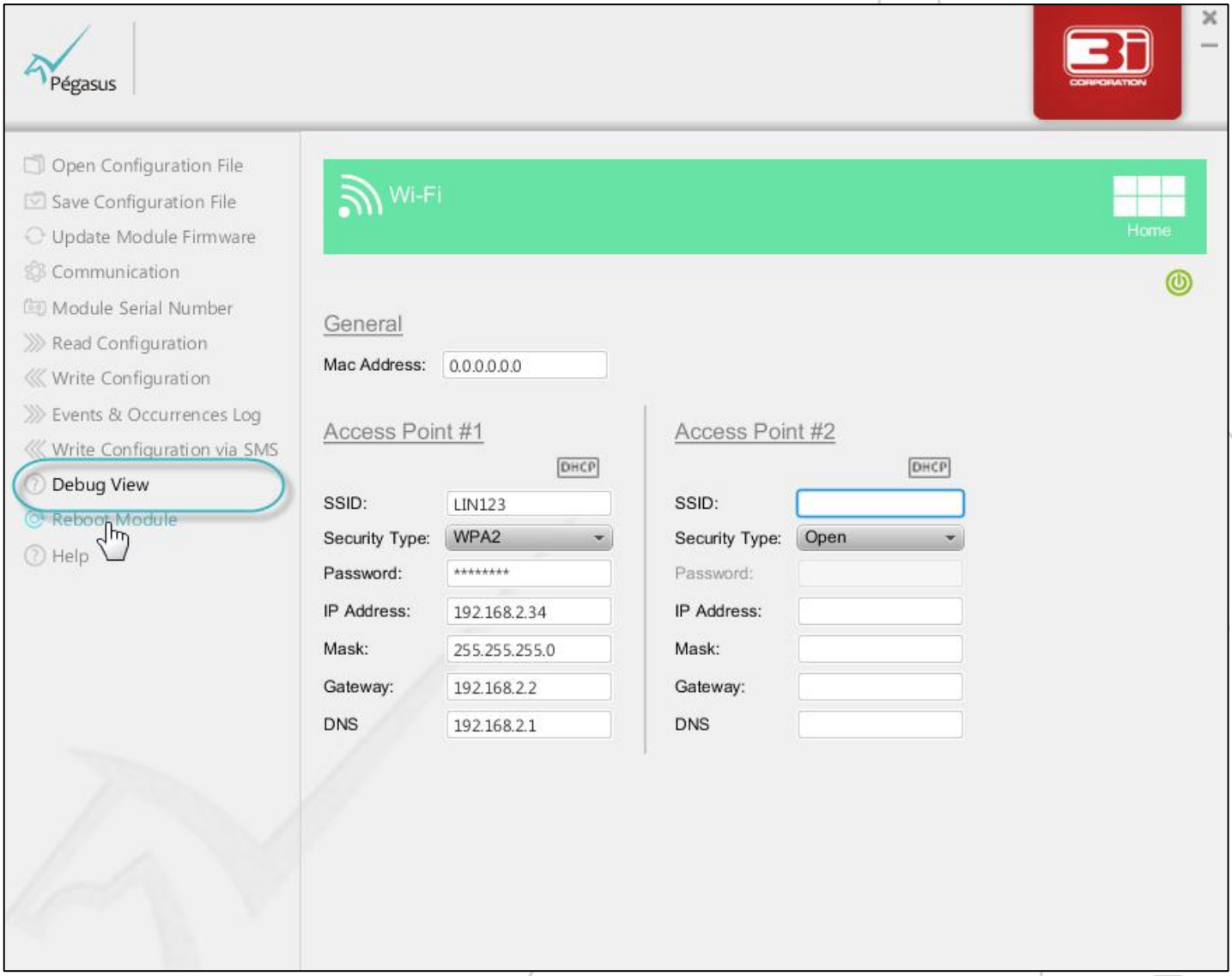


Note:

To learn how to write the configuration settings to Pegasus™ NX, refer the **Write Configuration** chapter.

6.7. Reboot Module

On successful writing of the Pegasus NX configfuration settings, to make all configured features functional, reboot of module is required.



Note:

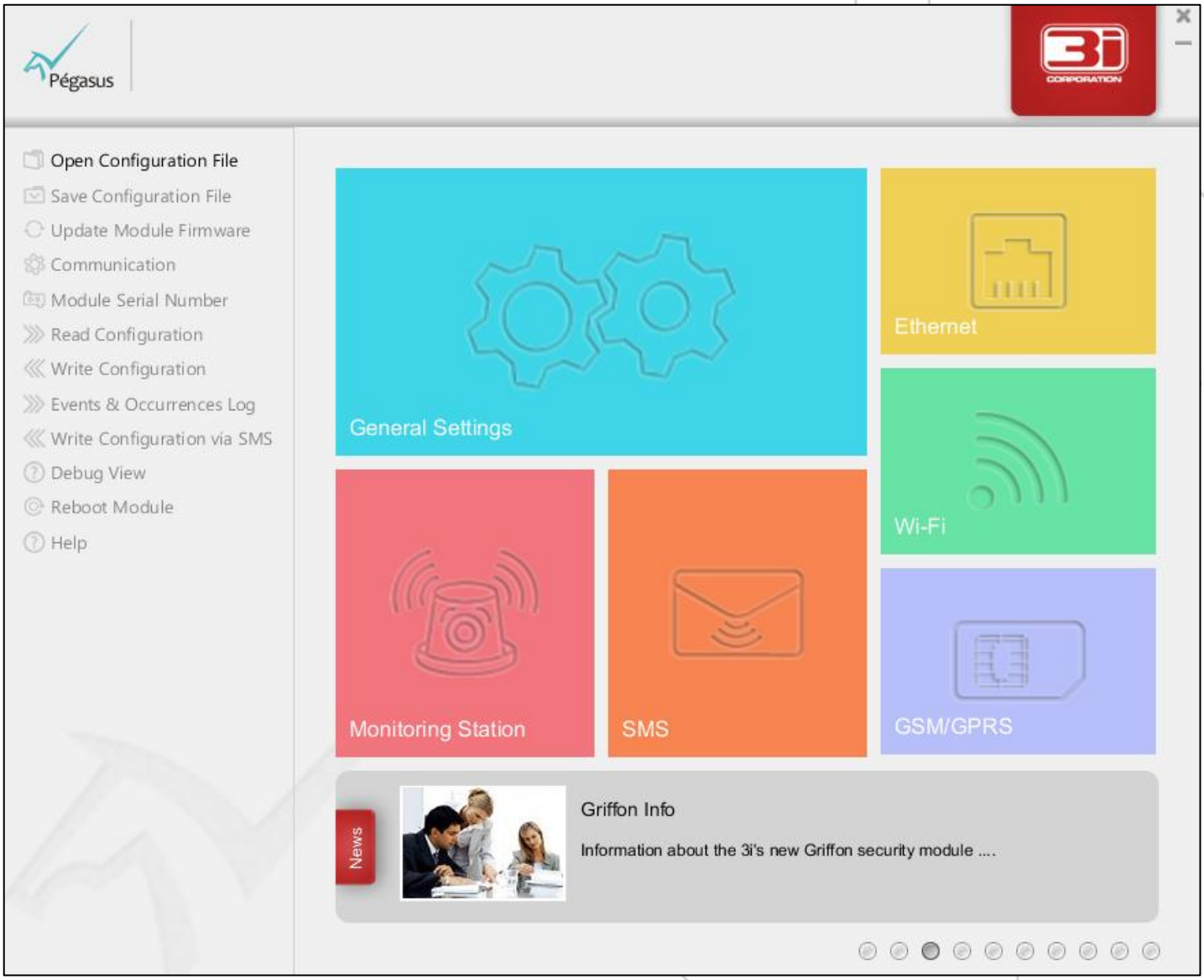
To learn how to reboot module after writing the configuration to Pegasus™ NX, refer the **Reboot Module** chapter.

6.8. Return Back to the Home Screen

To return back to the home screen

1. Click the **Home** icon as shown in the below image.

The **Pegasus™ Studio Home Screen** is displayed.



7 SMS

The **SMS** screen is built-in two interfaces: Incoming SMS and Outgoing SMS. The Incoming SMS interface allows you to enable/disable and configure from which numbers Pegasus™ NX is allowed to receive messages.

The Outgoing SMS interface allows you to enable/disable and configure the phone numbers which are allowed to receive messages related to events/occurrences.

Configuration Instructions

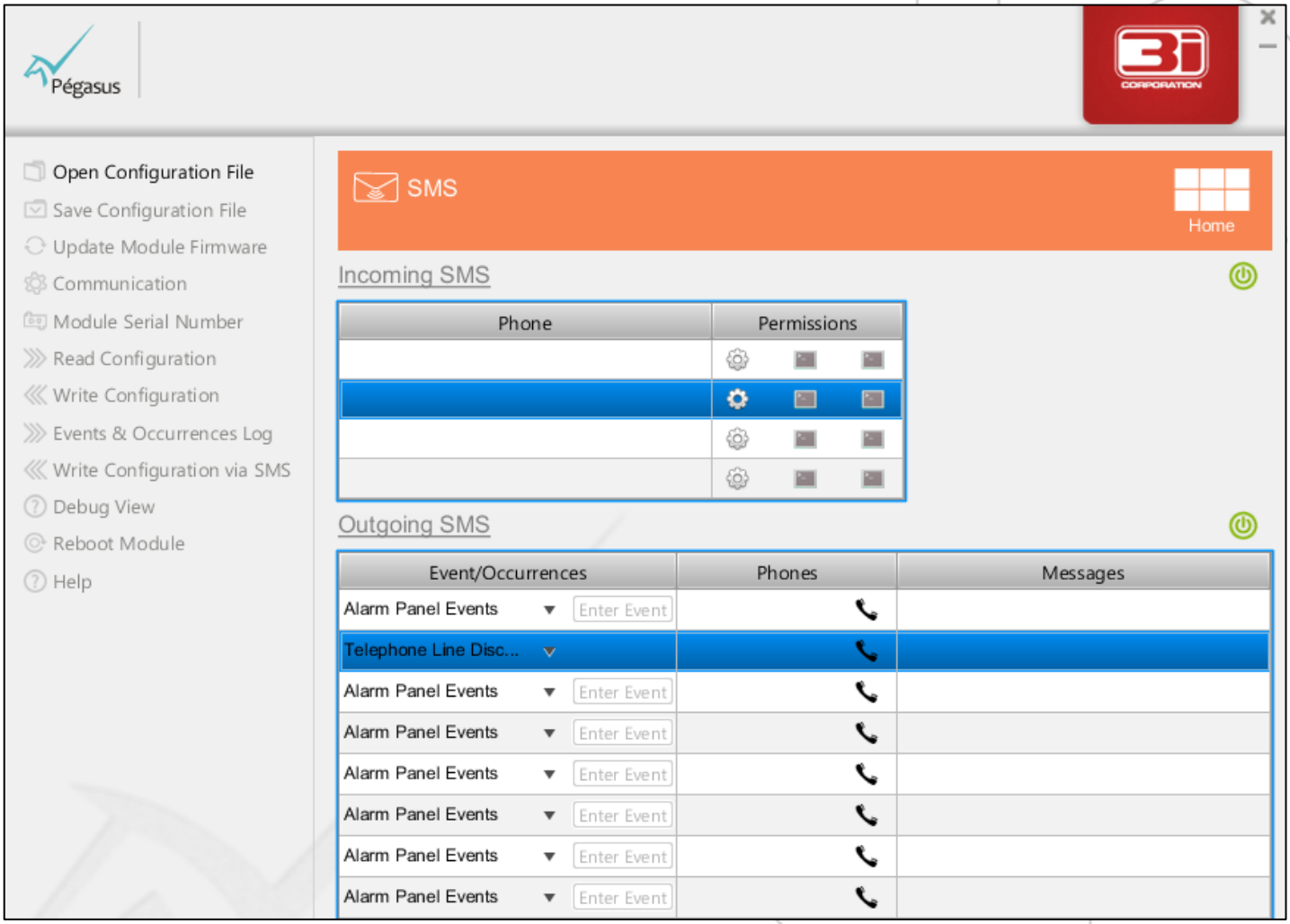
- To configure SMS, follow steps: 7.1 to 7.9.
- To configure Incoming SMS, follow steps: 7.2. Enable the Incoming SMS Interface, and 7.3. Configure Incoming SMS.
- To configure Outgoing SMS, follow steps: 7.4. Enable the Outgoing SMS Interface, and 7.5. Configure Outgoing SMS for Alarm Panel Event.
- To write the SMS configuration to Pegasus NX, follow step 7.7. Write Configuration. To apply the SMS configuration settings, follow step 7.8. Reboot Module.

7.1. Open the SMS Screen

To open the sms screen

1. On the **Pegasus™ Studio Main Screen**, place your cursor on the **SMS** section, and then click to open the **SMS** screen.

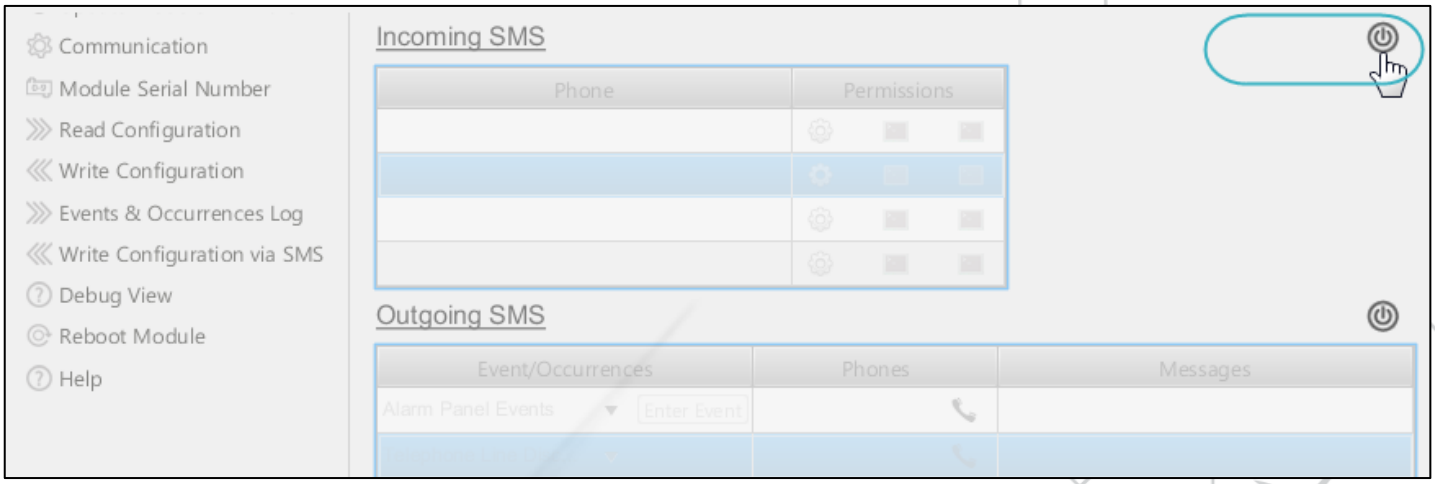
The **SMS** screen is displayed as shown below.



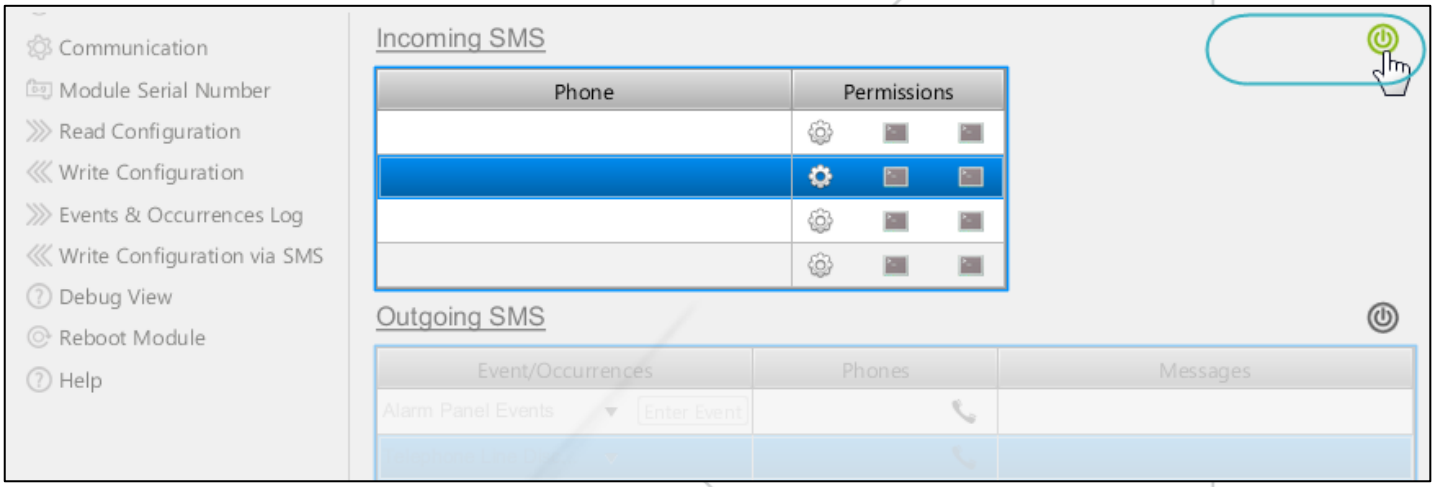
7.2. Enable the Incoming SMS Interface

Important Information:

To receive sms, the GSM/GPRS interface should be in the enabled state.



3. The grey colored icon is turned green  as shown in the below image. The SMS interface is in the enabled state.

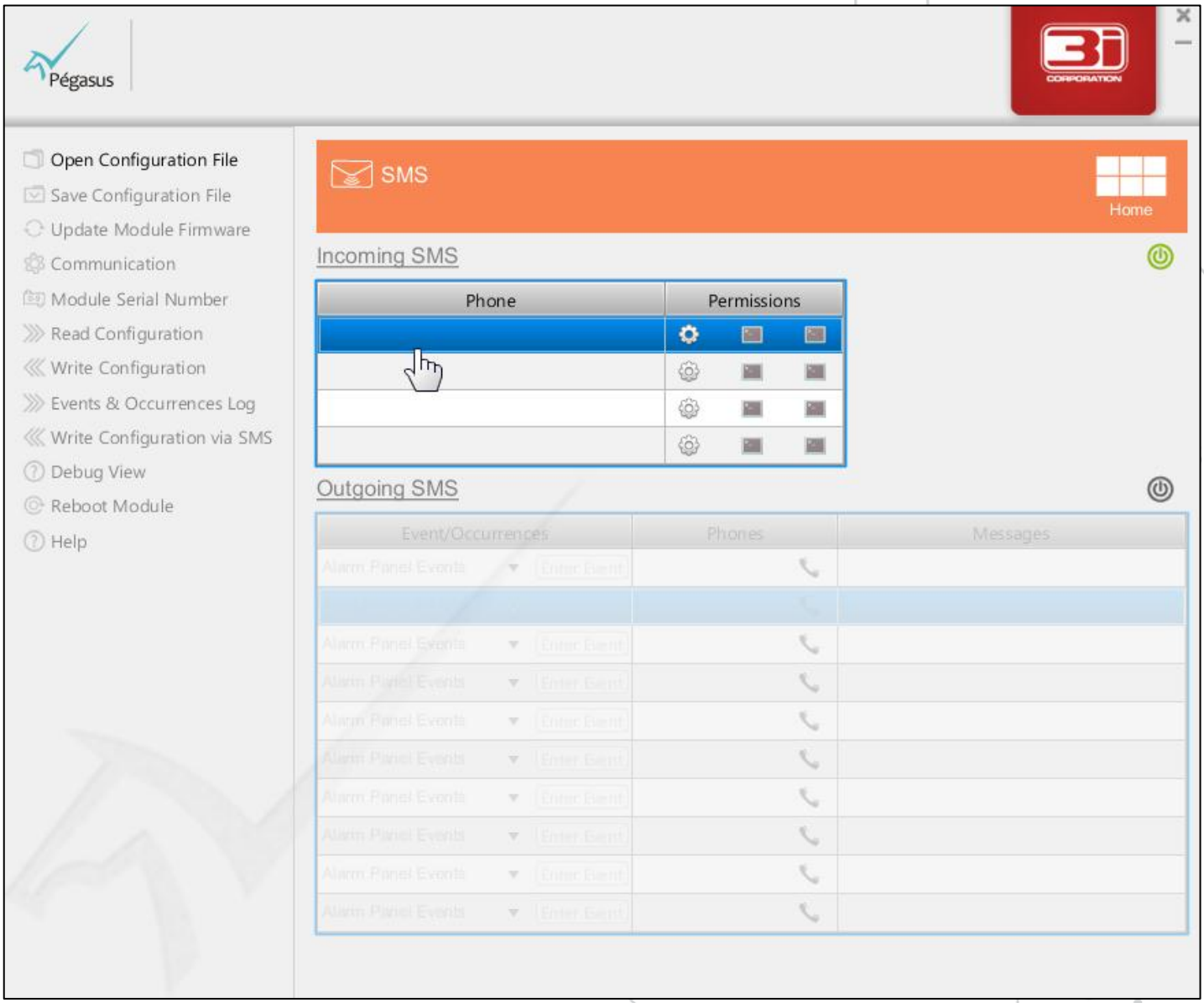


7.3. Configure Incoming SMS

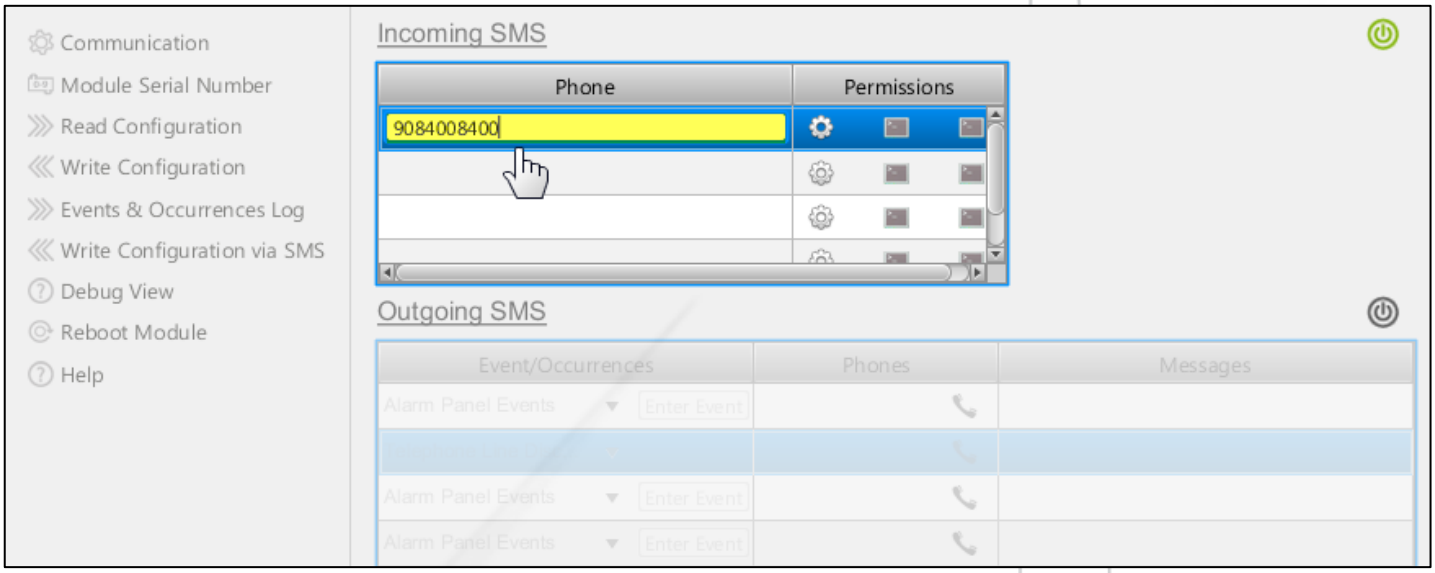
Incoming SMS allows you to configure upto four phone numbers from which Pegasus™ NX is allowed to receive messages.

To configure incoming sms

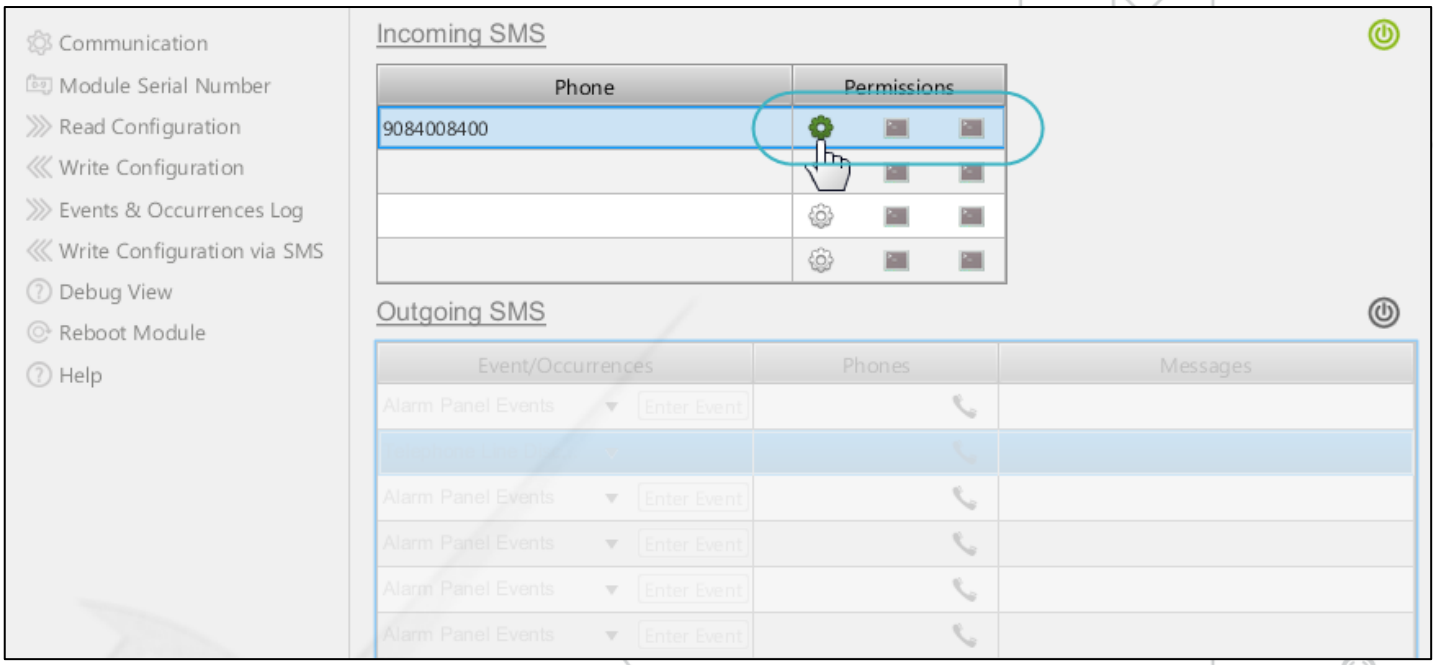
1. Under Incoming SMS, click to select the 1st row as shown in the below image.



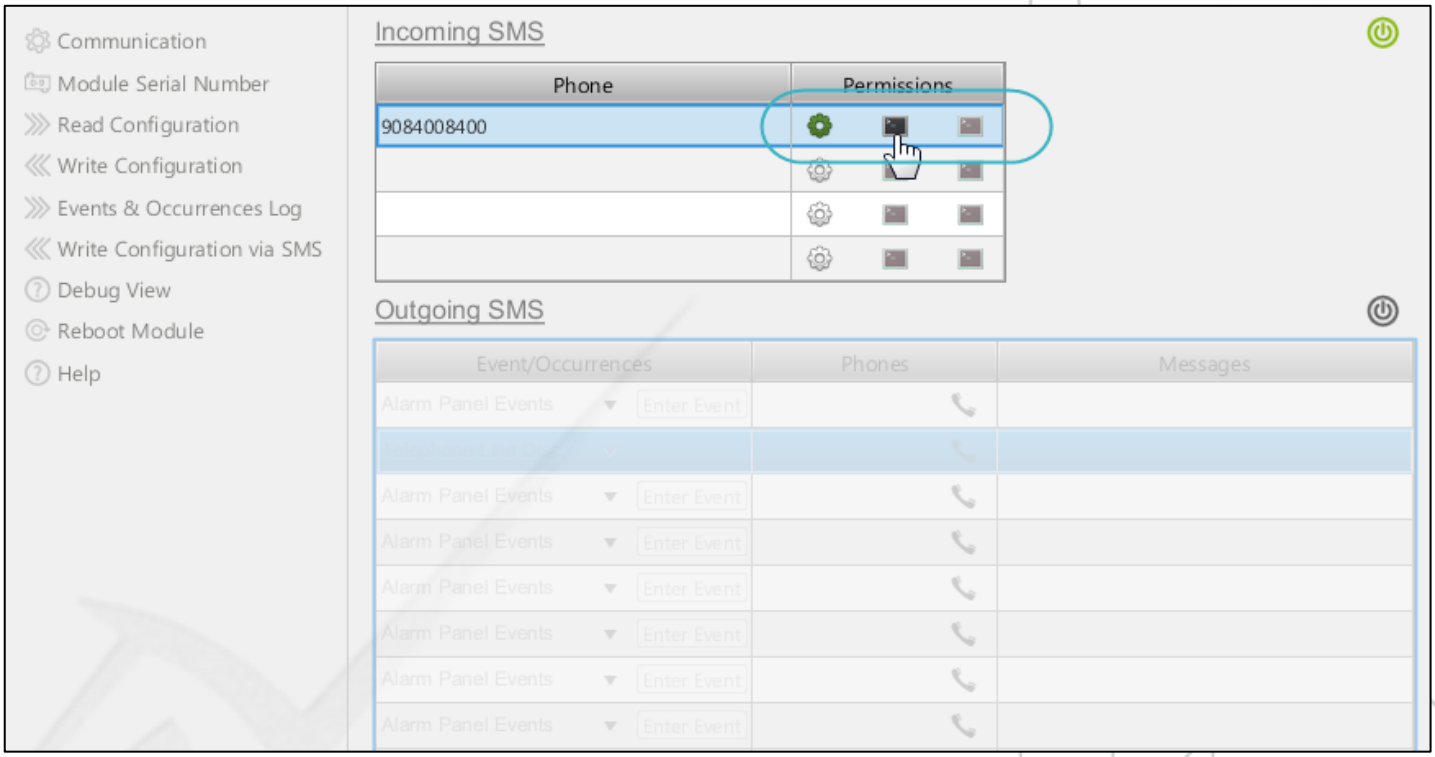
2. Under Phone, enter the **phone number** of the individual whose incoming sms will be accepted by the device.



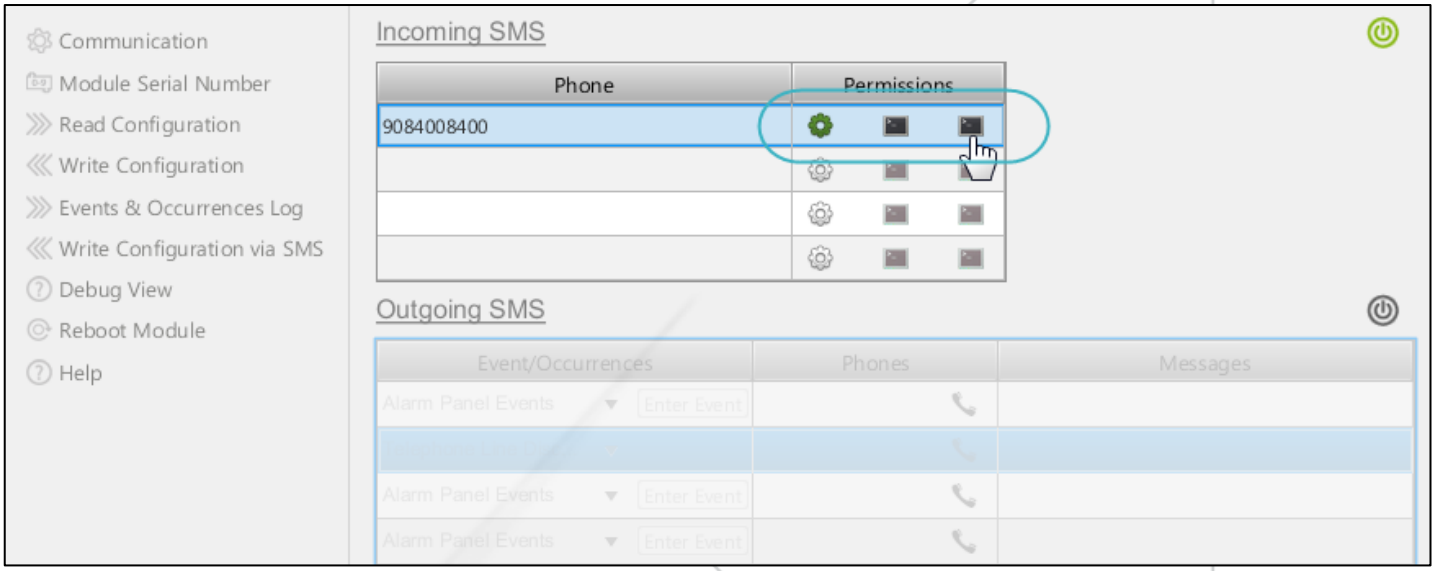
3. Under Permissions, click the **Configuration Update**  icon to provide permission for configuration update. The grey colored icon is turned green  as shown in the below image.



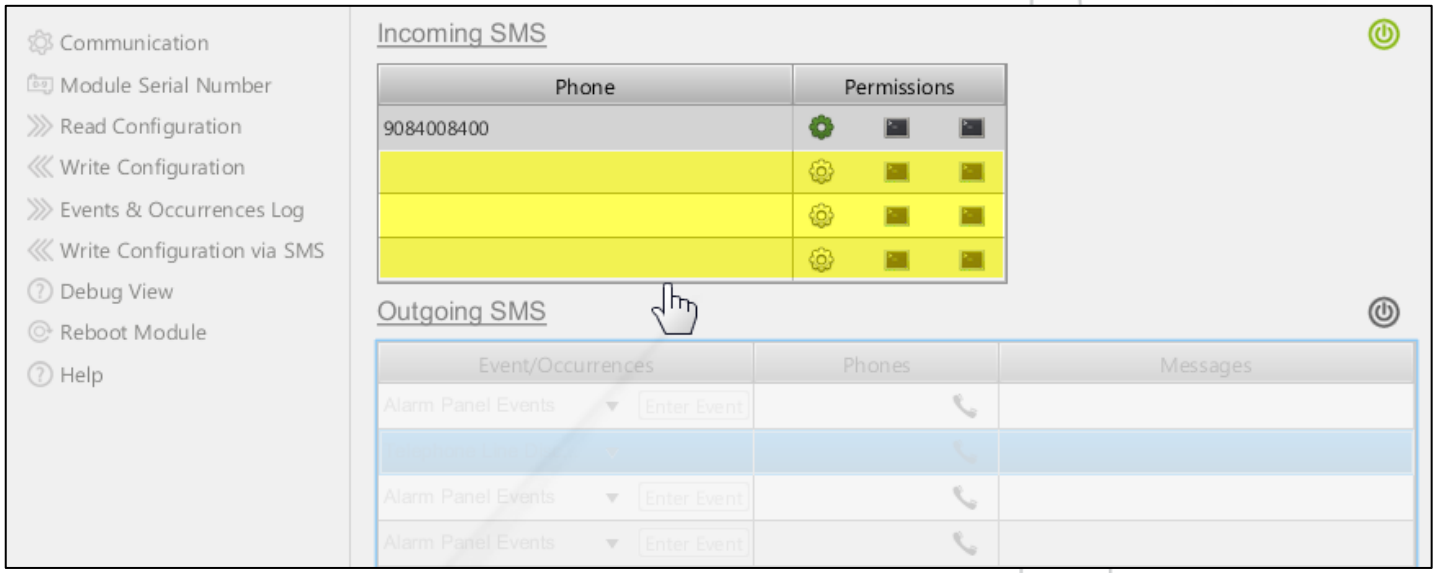
4. Under Permissions, click the **Remote Command**  icon to provide permission for remote command. The light grey colored icon is turned dark grey  as shown in the below image.



5. Under Permissions, click the **Echo**  icon to provide permission for echo. The light grey colored icon is turned dark grey  as shown in the below image.



6. Likewise, you can configure incoming sms for phone numbers: 2, 3 and 4. You can also provide permissions for configuration update, remote command, and/or echo.

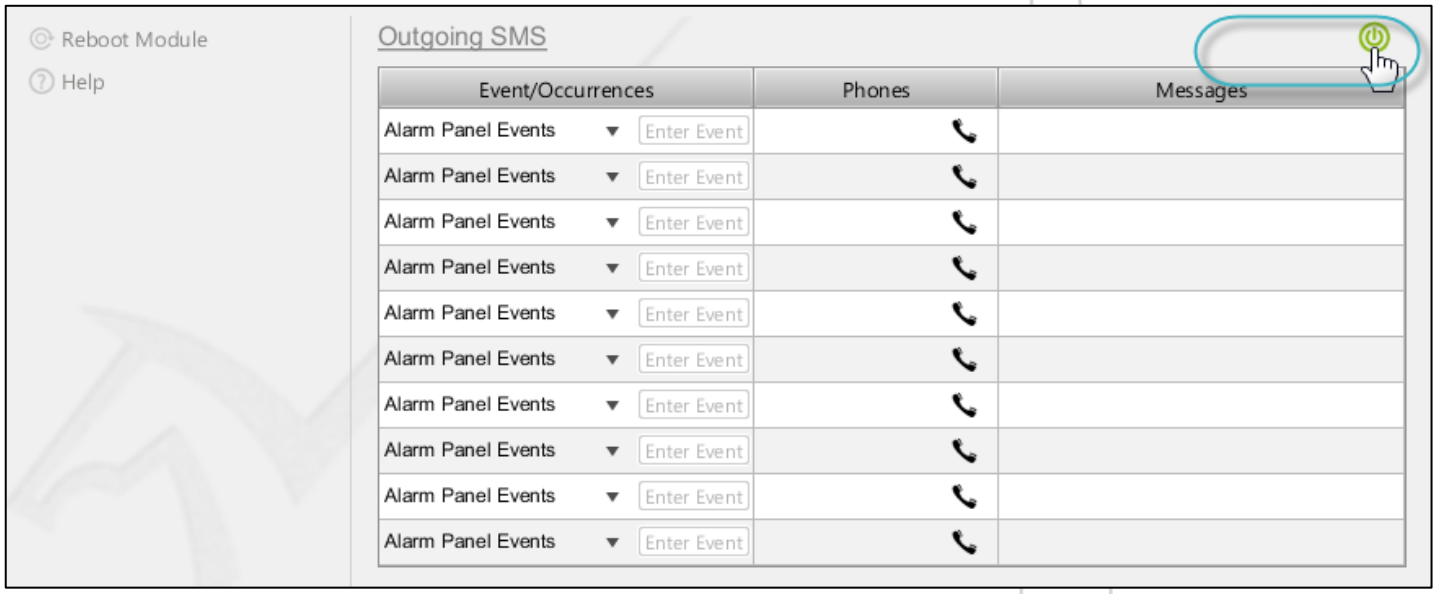


7.4. Enable the Outgoing SMS Interface

To enable the outgoing sms interface

1. Click the grey colored **Enable Outgoing SMS**  icon.

The grey colored icon is turned green  as shown in the below image. The Outgoing SMS interface is now in the enabled state.

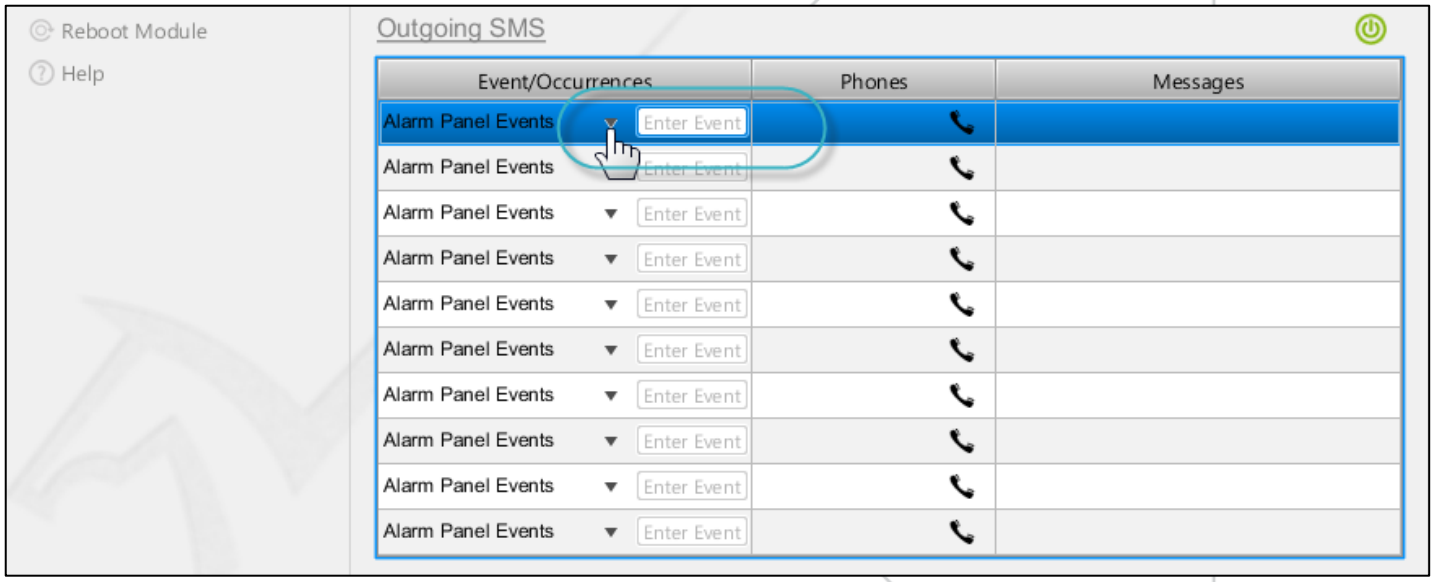


7.5. Configure Outgoing SMS for Alarm Panel Event

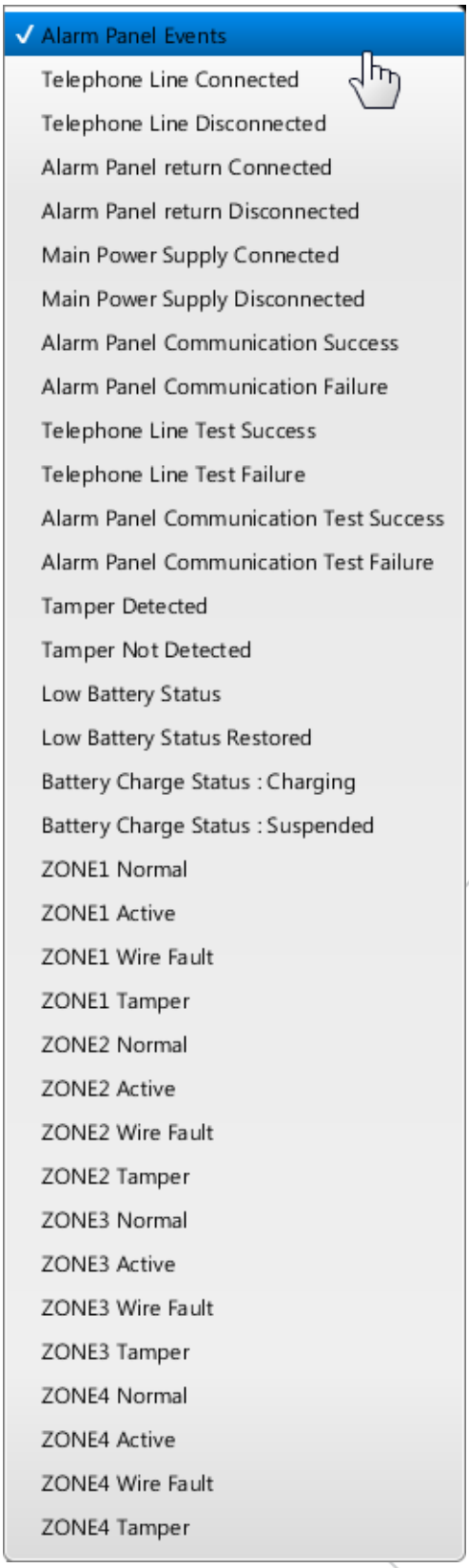
The Outgoing SMS interface allows you to configure upto four phone numbers which are allowed to receive the configured message to each event/occurrence. Outgoing messages to total 10 events/occurrences can be configured and each message can be sent to upto four configured phone numbers.

To configure outgoing sms for alarm panel event

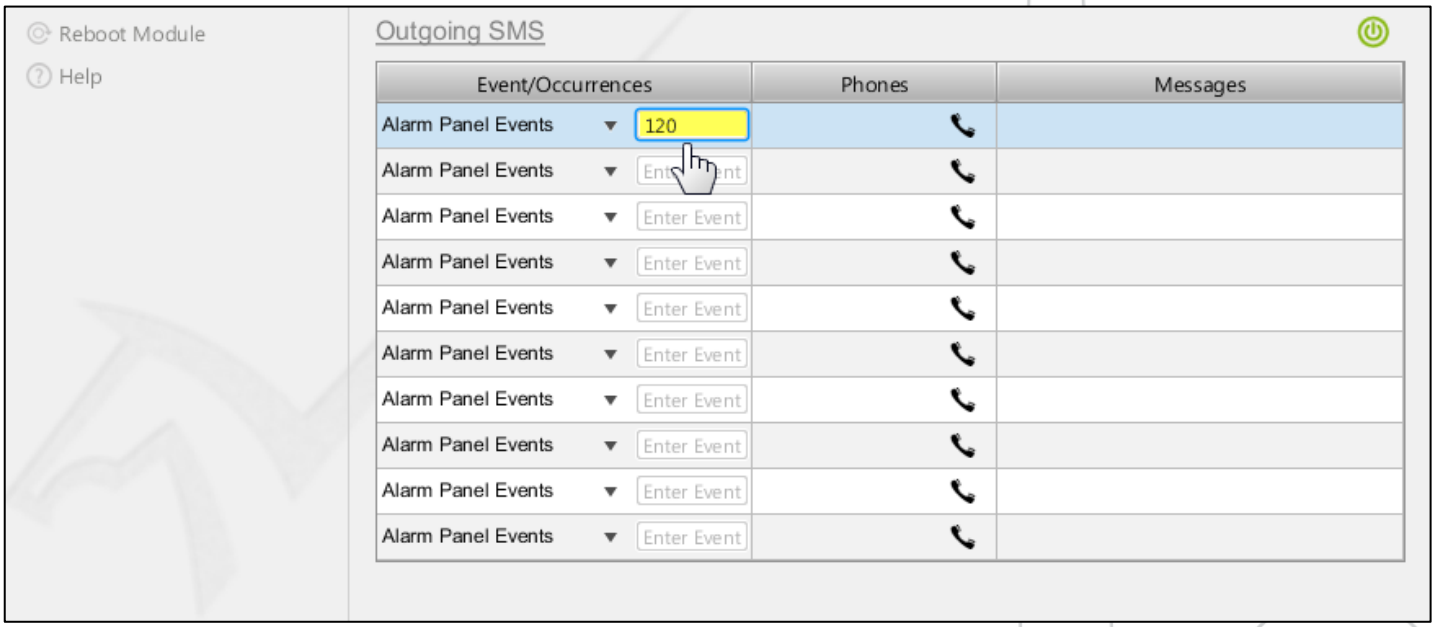
1. Under Event/Occurrences, click the drop-down arrow as shown in the below image.



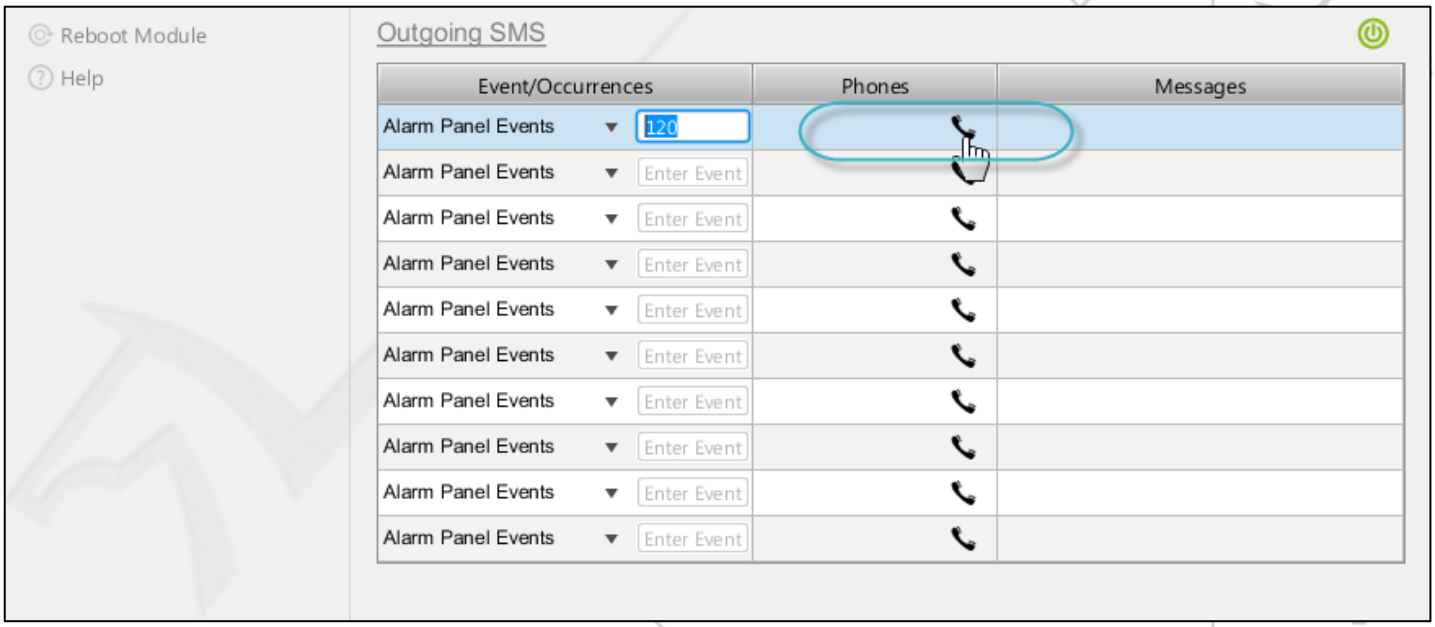
2. A menu with alarm panel event and occurrences is displayed. Select the **Alarm Panel Events** option.



3. In the **Enter Event** text box, enter the three digit **Event Code** as per the Contact ID Protocol.



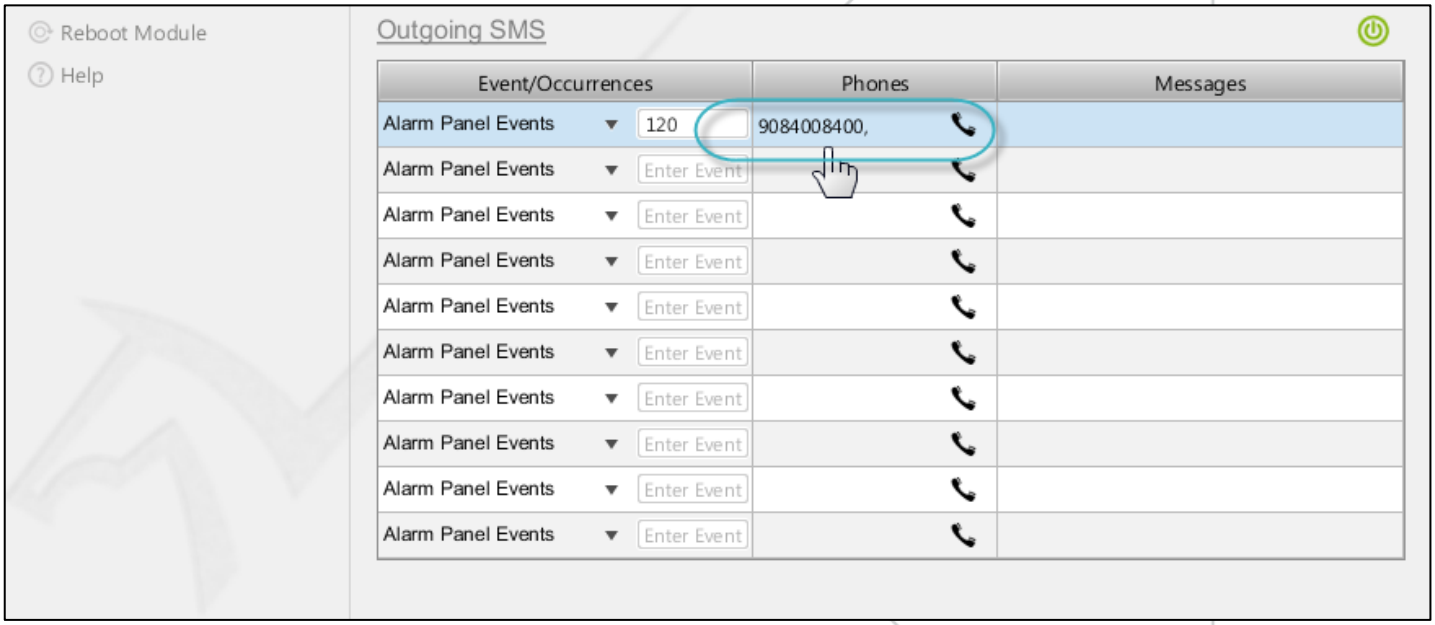
4. Click the **Phone**  icon as shown in the below image.



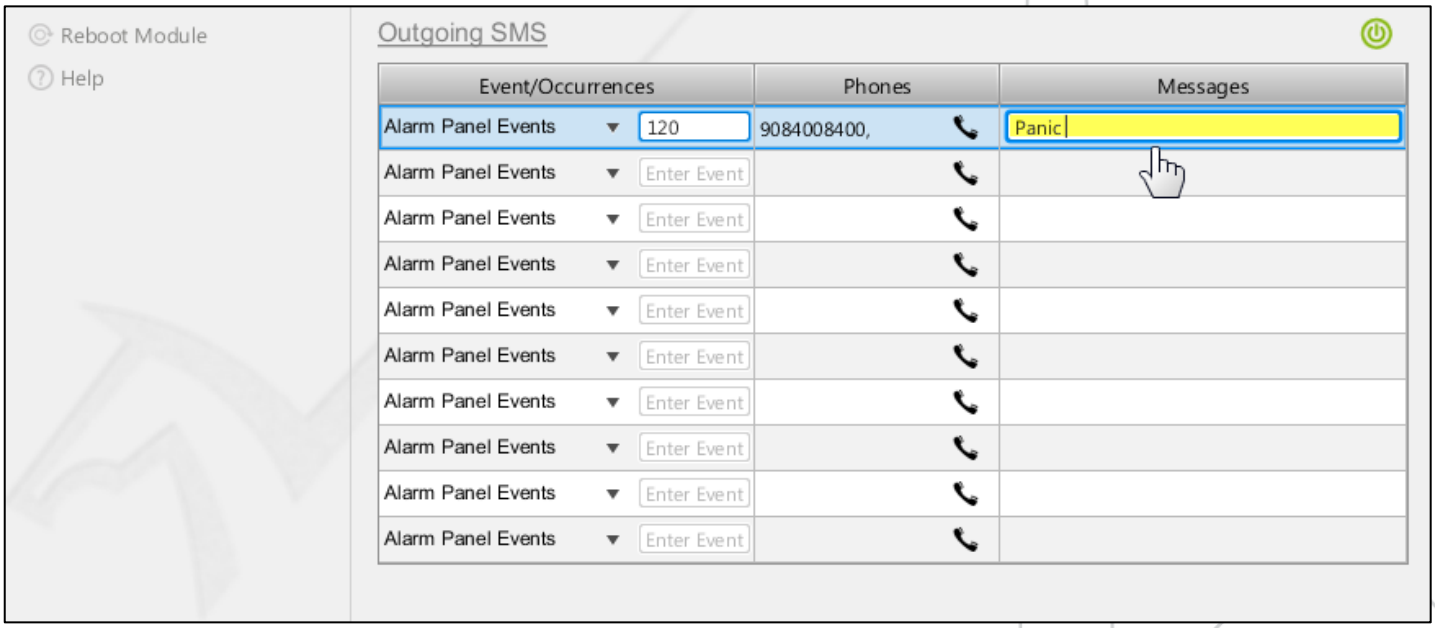
5. The **Phones** dialog box is displayed. In this dialog box, you can enter upto four phone numbers. In **Phone #1** text box, enter the 1st phone number which will receive the configured event message as shown in the below image.

6. Click the **OK** button.

7. Under **Phones**, the phone number is displayed as shown in the below image.



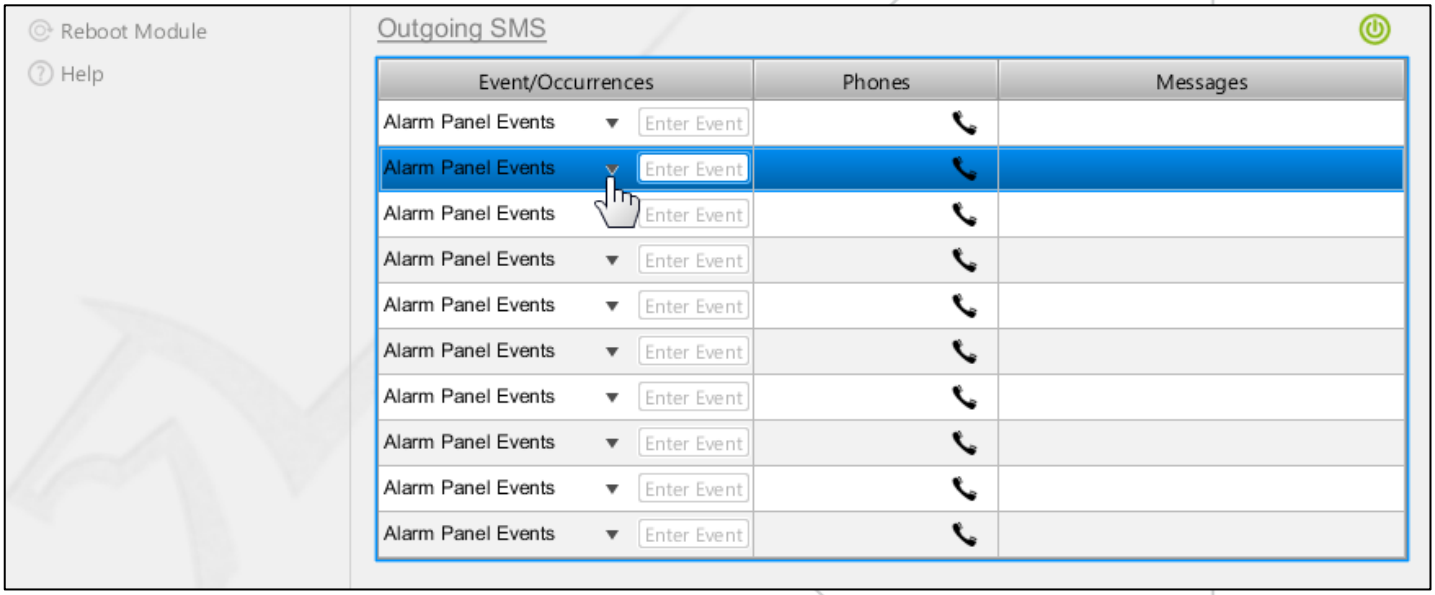
8. Under Messages, type-in the **Event Message**. This message will be sent to the configured phone number whenever the related event occurs.



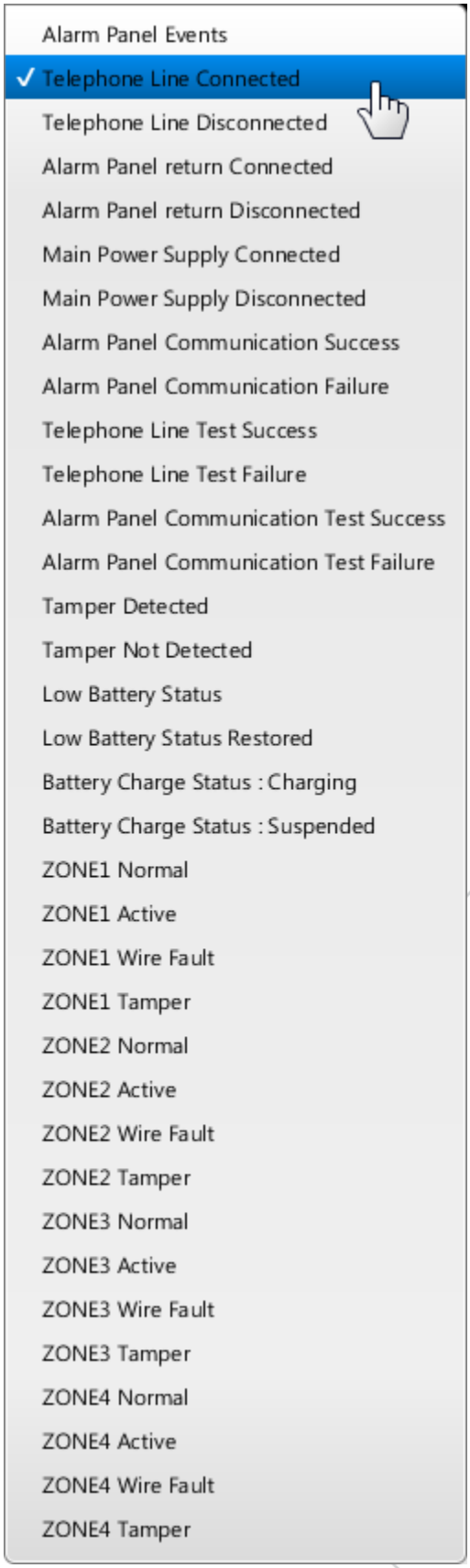
7.6. Configure Outgoing SMS for Occurrences

To configure outgoing sms for occurrences

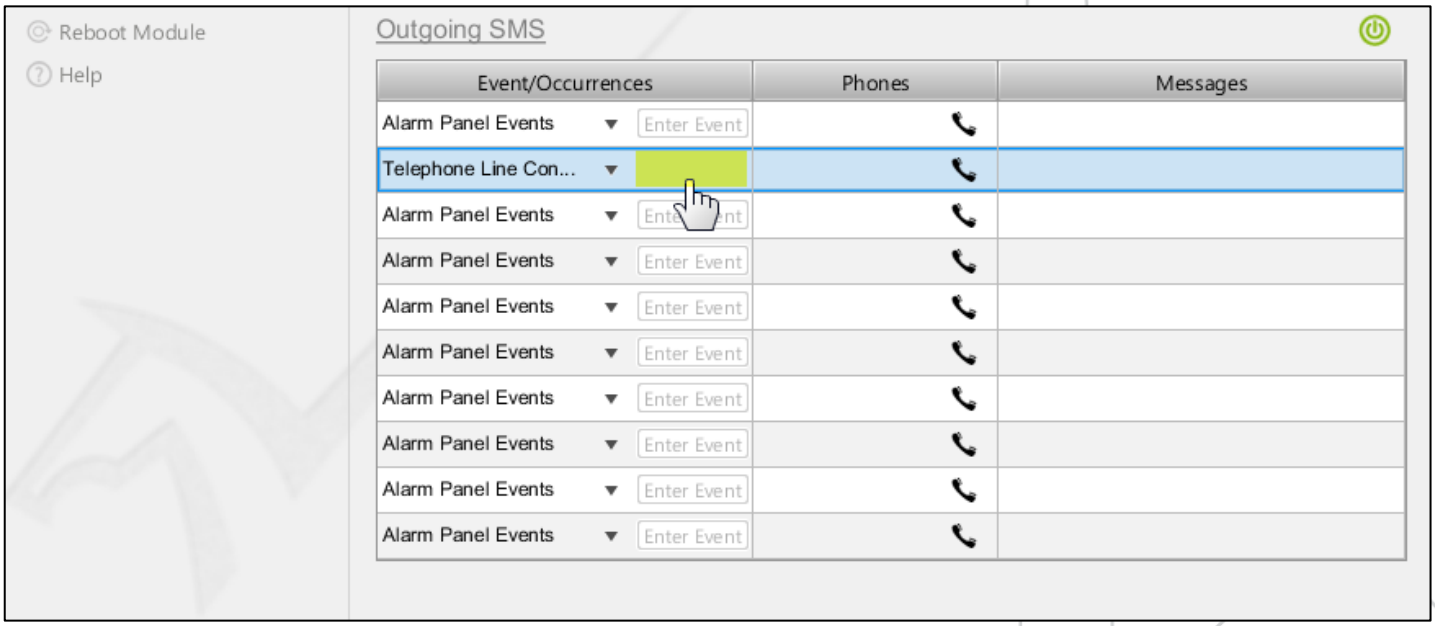
1. Under Event/Occurrences, click the drop-down arrow as shown in the below image.



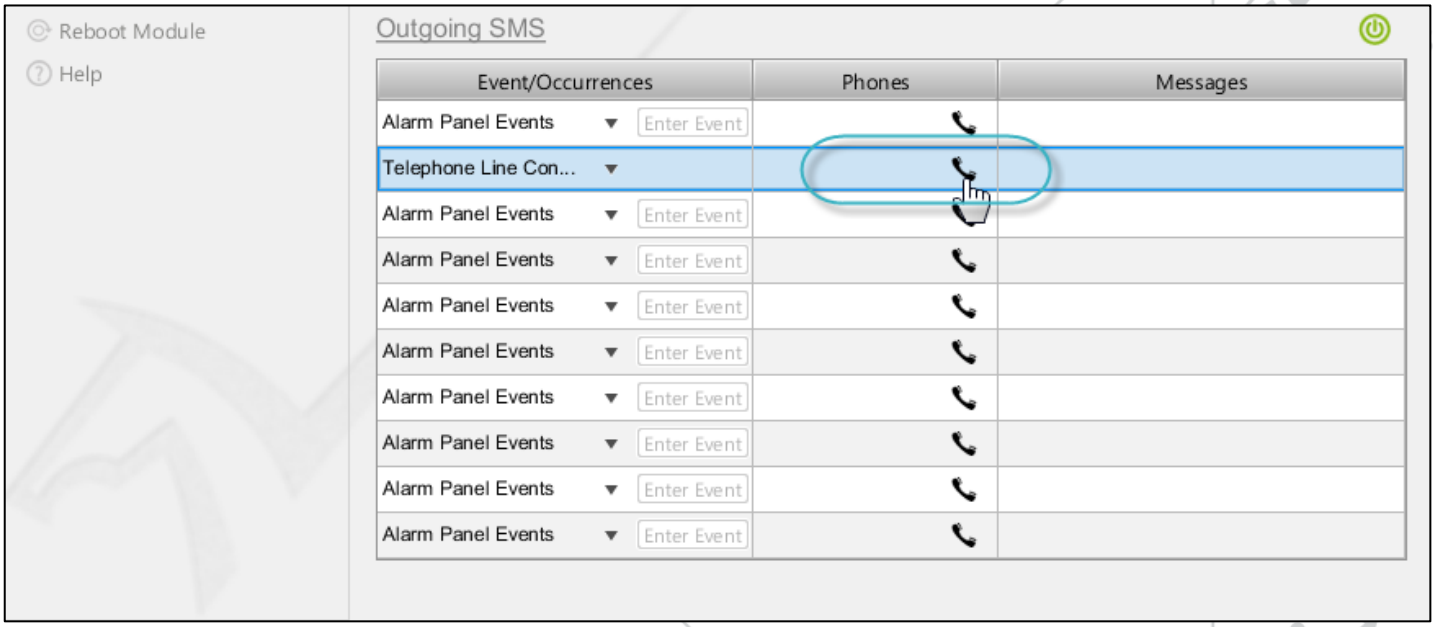
2. A menu with one Alarm Panel Events option and 42 Occurrences is displayed. Select an **Occurrance**.


Alarm Panel Events
Telephone Line Connected
Telephone Line Disconnected
Alarm Panel return Connected
Alarm Panel return Disconnected
Main Power Supply Connected
Main Power Supply Disconnected
Alarm Panel Communication Success
Alarm Panel Communication Failure
Telephone Line Test Success
Telephone Line Test Failure
Alarm Panel Communication Test Success
Alarm Panel Communication Test Failure
Tamper Detected
Tamper Not Detected
Low Battery Status
Low Battery Status Restored
Battery Charge Status : Charging
Battery Charge Status : Suspended
ZONE1 Normal
ZONE1 Active
ZONE1 Wire Fault
ZONE1 Tamper
ZONE2 Normal
ZONE2 Active
ZONE2 Wire Fault
ZONE2 Tamper
ZONE3 Normal
ZONE3 Active
ZONE3 Wire Fault
ZONE3 Tamper
ZONE4 Normal
ZONE4 Active
ZONE4 Wire Fault
ZONE4 Tamper

Once you select the occurrence, the **Enter Event** text box is disappeared as entry of an Event code is not required for an occurrence.



3. Click the **Phone**  icon as shown in the below image.

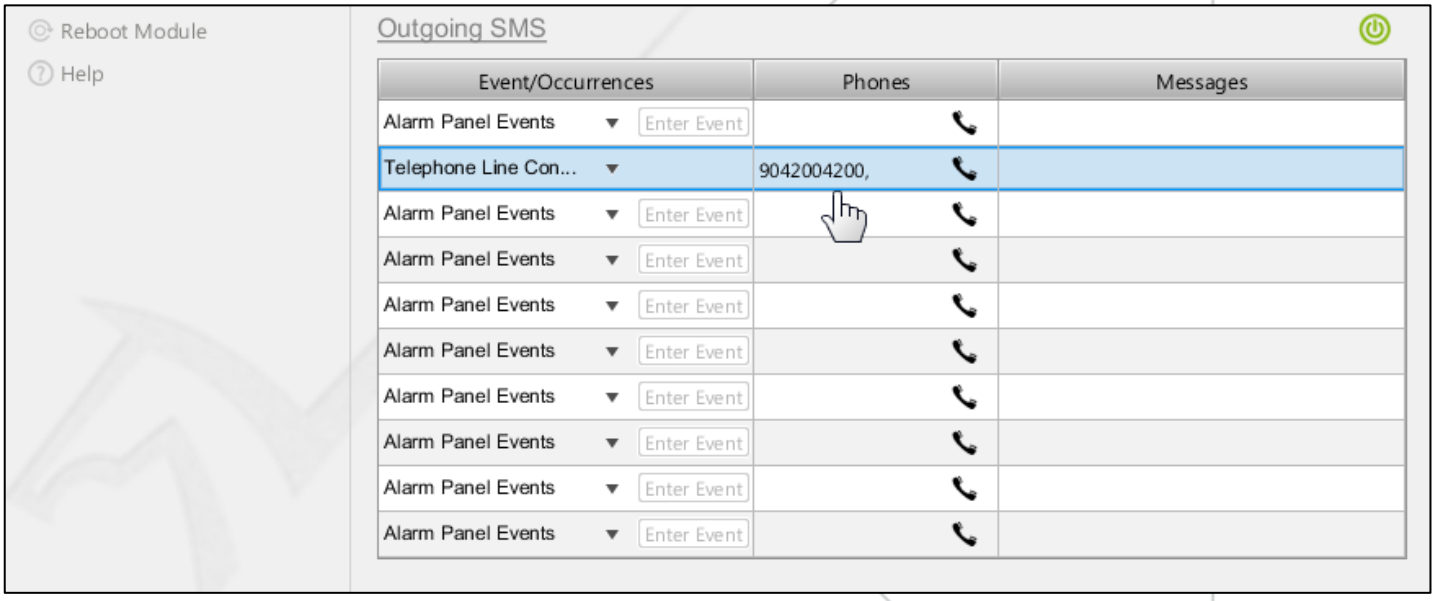


The **Phones** dialog box is displayed.

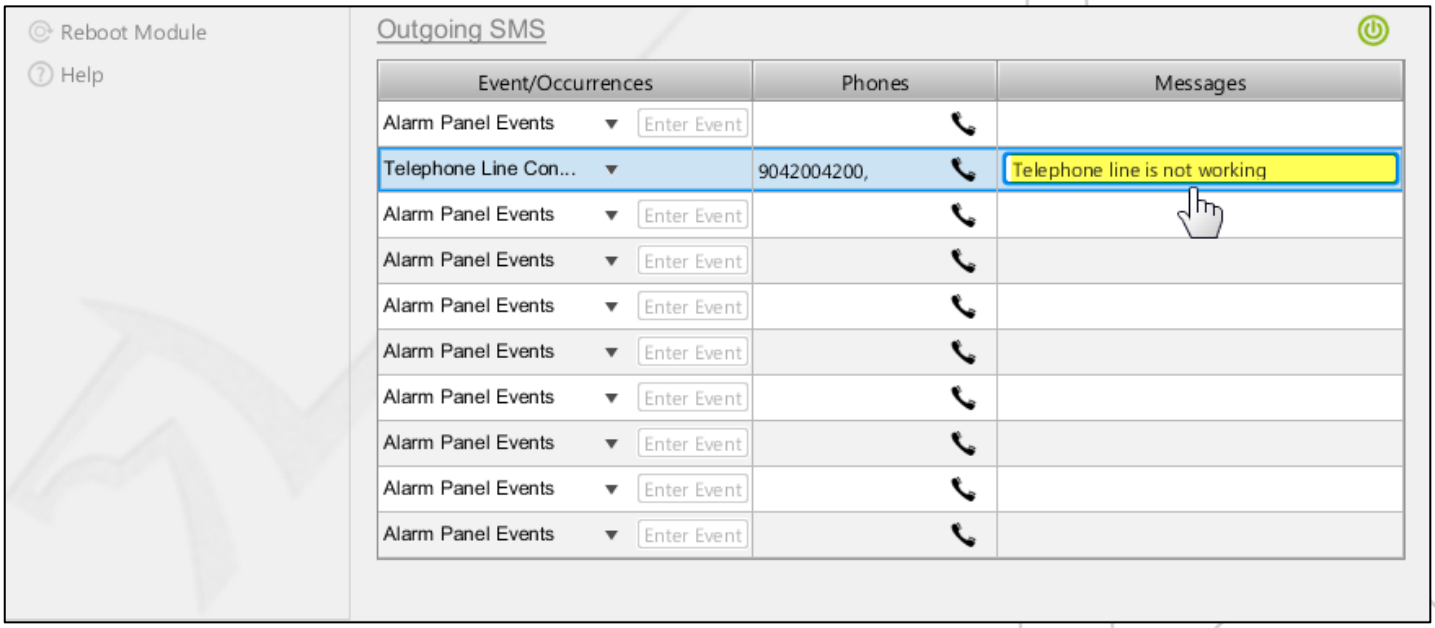
4. In **Phone #1** text box, enter the 1st phone number which will receive the occurrence message as shown in the below image.

5. Click the **OK** button.

6. Under **Phones**, the phone number is displayed as shown in the below image.

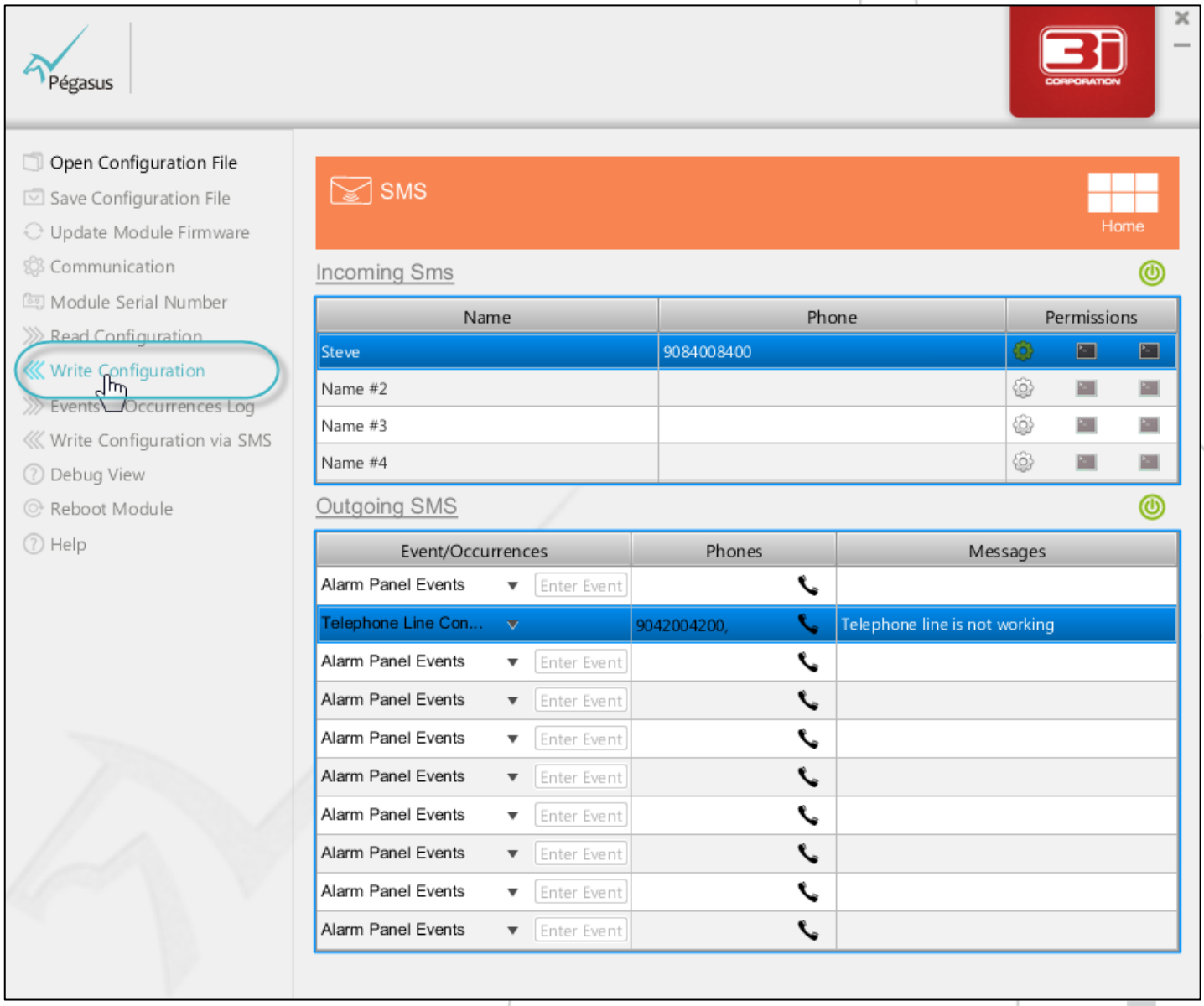


7. Under Messages, type-in the **Occurrence Message**. This message will be sent to the configured phone number whenever the related occurrence occurs.



7.7. Write Configuration

When the incoming/outgoing SMS configuration settings are done, write configuration to Pegasus™ NX.

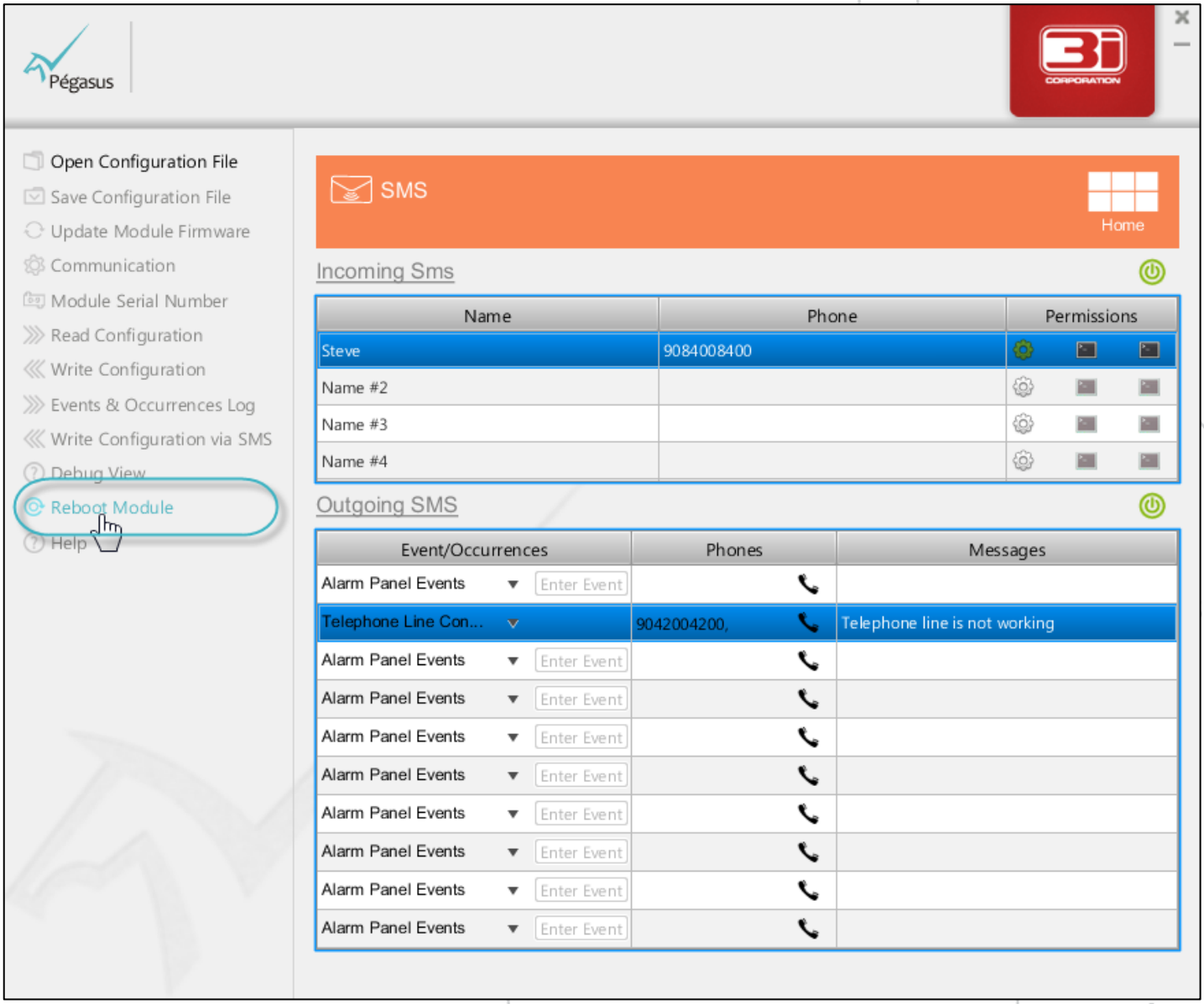


Note:

To learn how to write the configuration settings to Pegasus™ NX, refer the **Write Configuration** chapter.

7.8. Reboot Module

On successful writing of the Pegasus NX configfuration settings, to make all configured features functional, reboot of module is required.



Note:

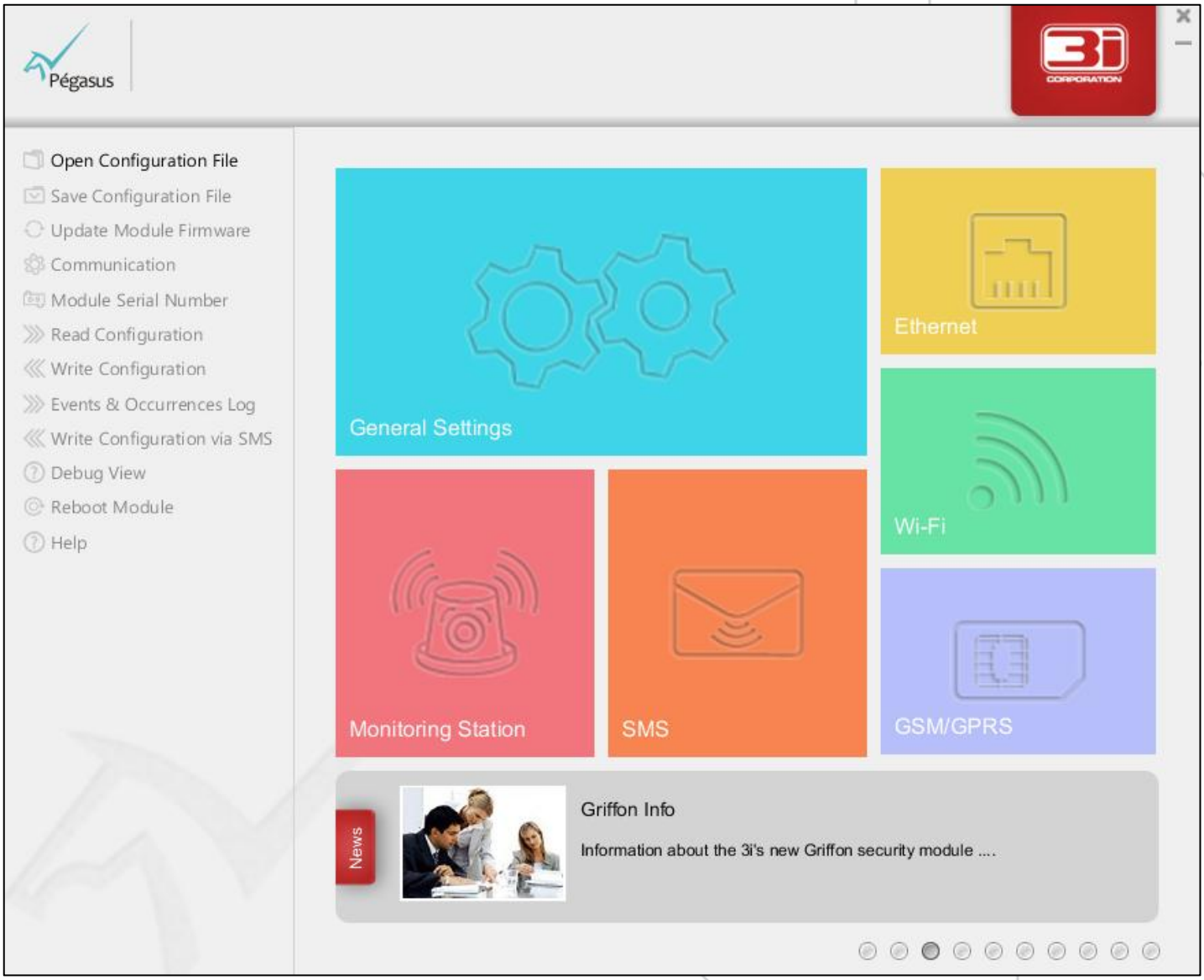
To learn how to reboot module after writing the configuration to Pegasus™ NX, refer the **Reboot Module** chapter.

7.9. Return Back to the Home Screen

To return back to the home screen

2. Click the **Home** icon as shown in the below image.

The **Pegasus™ Studio Home Screen** is displayed.



8 Monitoring Station

The **Monitoring Station** screen allows you to configure settings related to the communication between Pegasus™ NX and the monitoring station using IP, GSM, CSD, SMS, etc.

Configuration Instructions

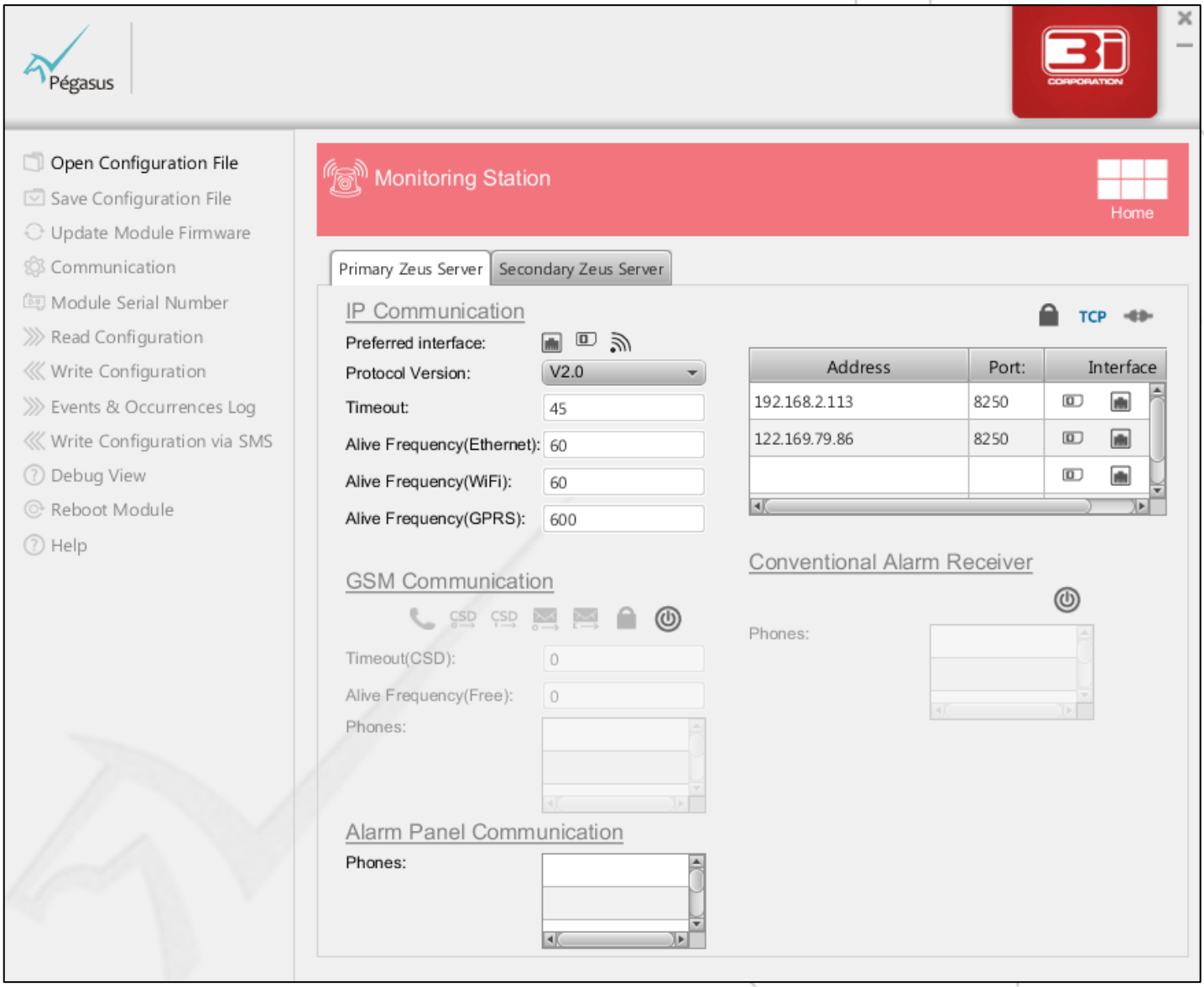
- To configure Monitoring Station, follow steps: 8.1 to 8.6.
- To configure GSM Communication, follow step 8.2.2. Configure GSM Communication. To configure the Conventional Alarm Receiver, follow step 8.2.4. Configure Conventional Alarm Receiver.
- To write the Monitoring Station configuration to Pegasus NX, follow step 8.4. Write Configuration. To apply the Monitoring Station configuration settings, follow step 8.5. Reboot Module.

8.1. Open the Monitoring Station Screen

To open the monitoring station screen

1. On the **Pegasus™ Studio Main Screen**, place your cursor on the **Monitoring Station** section, and then click to open the **Monitoring Station** screen.

The **Monitoring Station** screen is displayed as shown below.

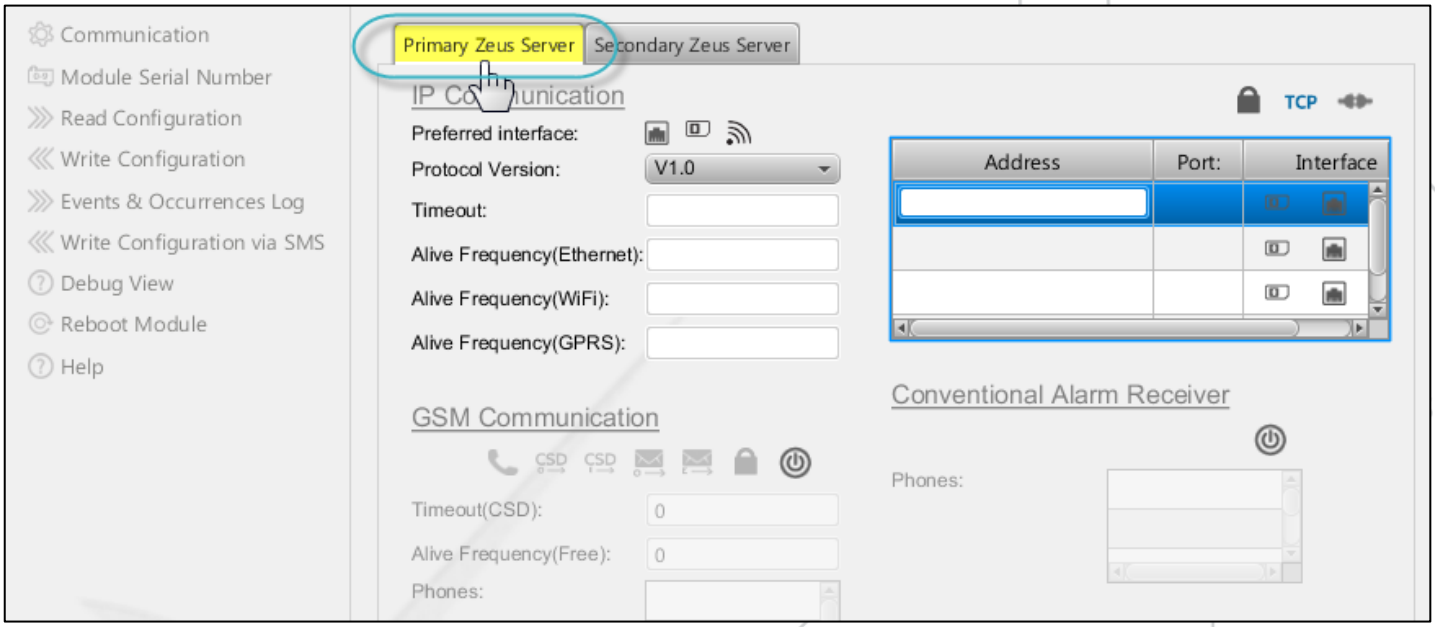


8.2. Configure Primary Zeus™ Server

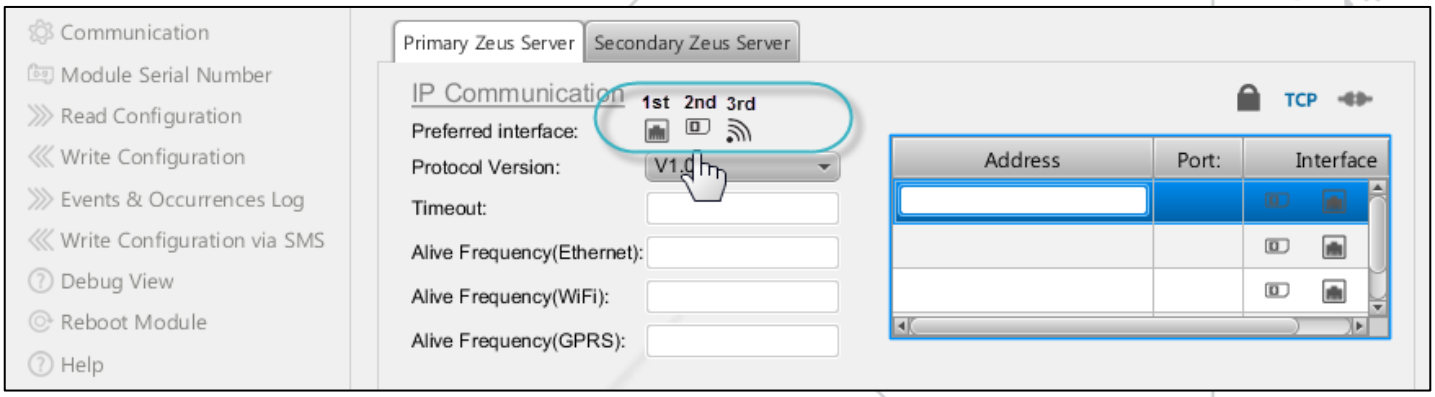
8.2.1. Configure IP Communication

To configure IP communication

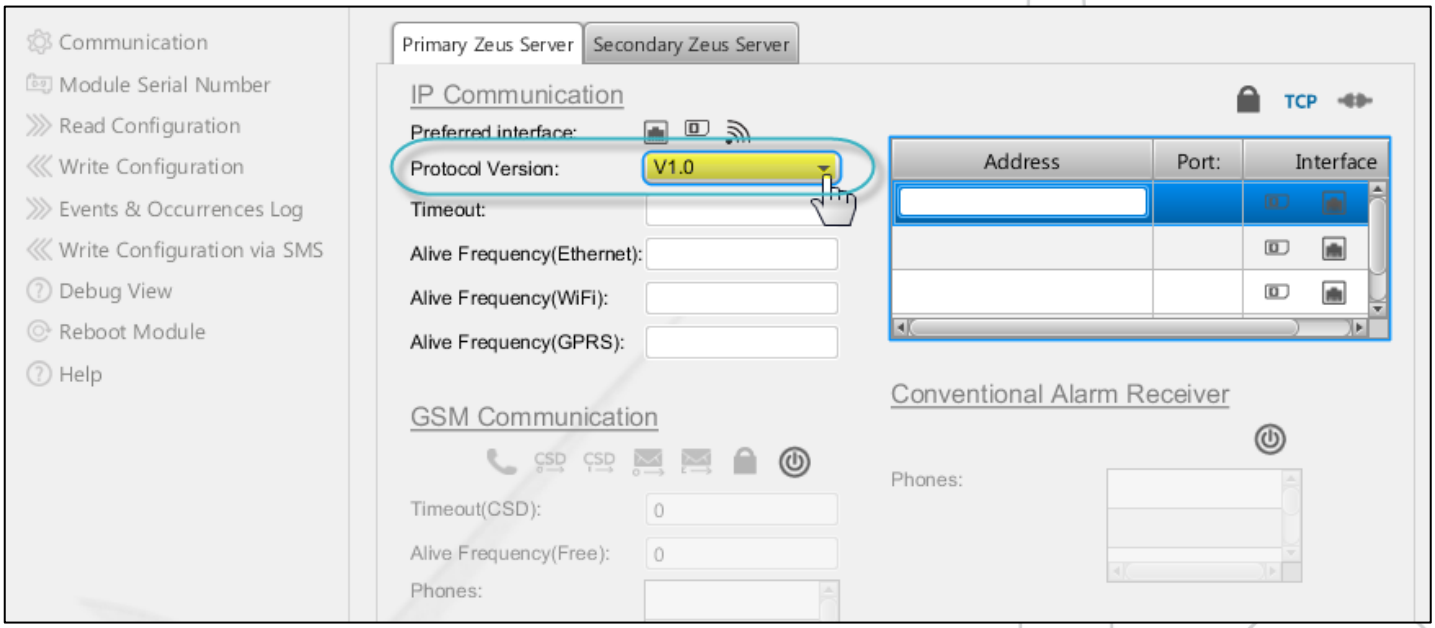
1. Click the **Primary Zeus™ Server** tab.



2. Under **Preferred Interface**, place the mouse pointer on any icon, left-click the mouse, and then drag-and-drop it horizontally at the first position (primary preferred interface), or the second position (secondary preferred interface), or the third position (tertiary preferred interface) as shown in the below image.

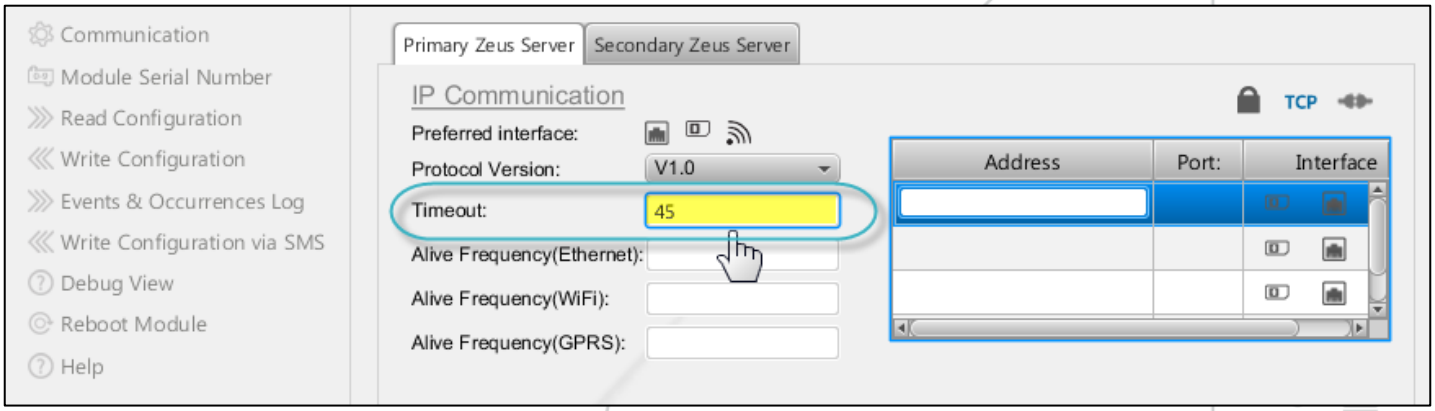


3. In the **Protocol Version** drop-down box, select the **Zeus™ Server Protocol Version** as **1.0** or **2.0**.



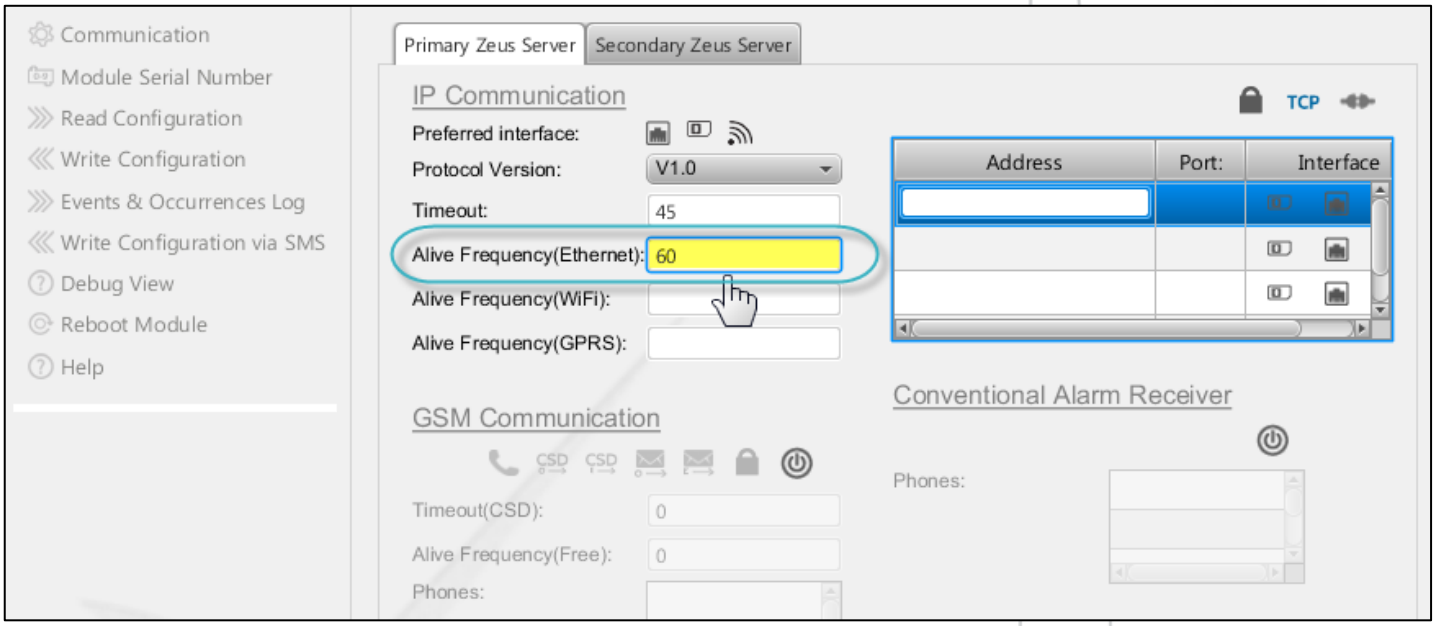
4. In the **Timeout** text box, enter your Pegasus™ Modules communication break time with the Primary Zeus™ Server in seconds.

   The minimum acceptable timeout duration is 15 seconds and the maximum acceptable timeout duration is 180 seconds. The default timeout duration is 30 seconds.



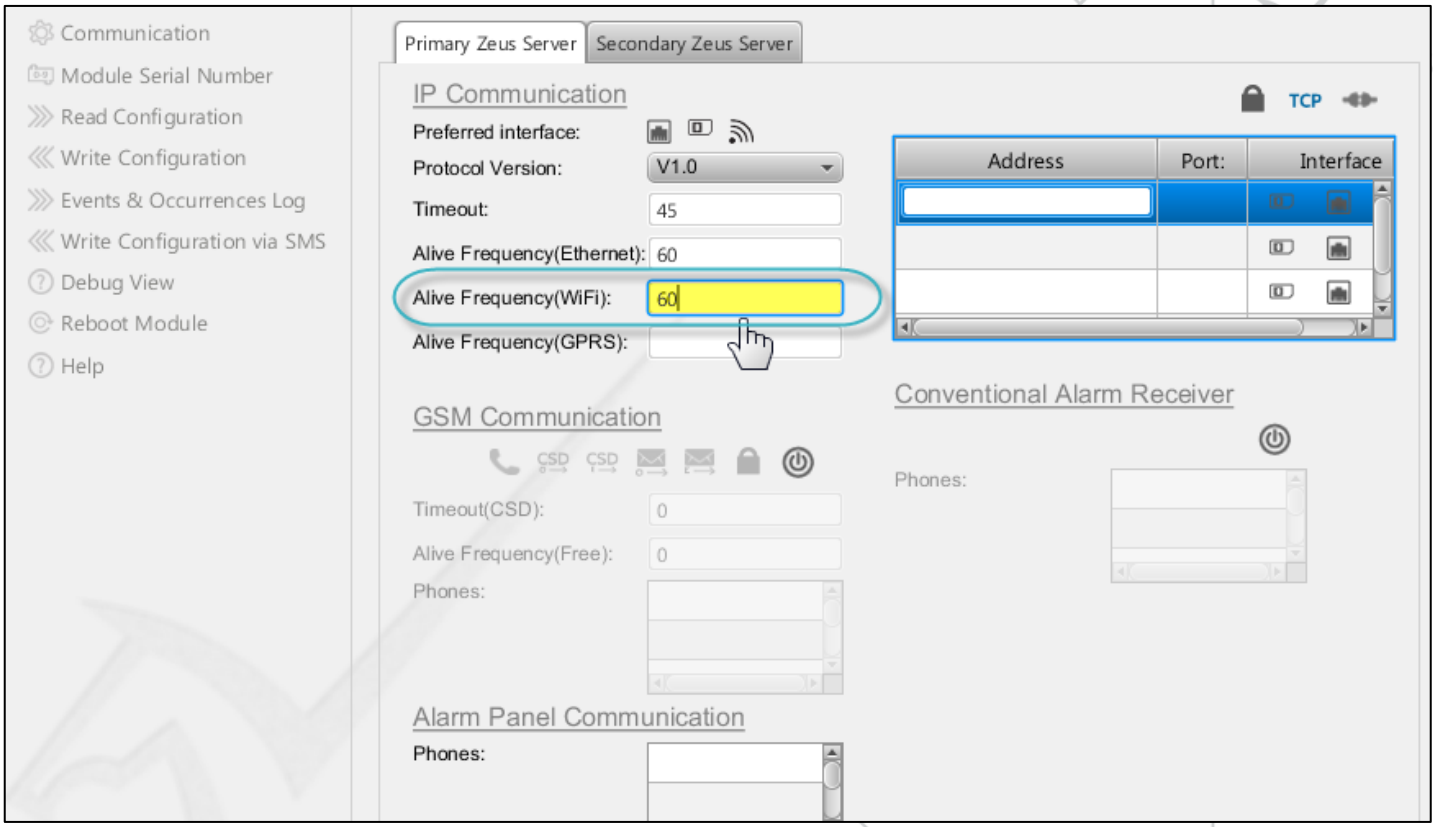
5. In the **Alive Frequency (Ethernet)** text box, enter the **Active Frequency of Ethernet** in seconds. Here, Pegasus™ NX sends identification/alive packets (Protocol v1.0) or M2S (Protocol v2.0) to the Primary Zeus™ Server via Ethernet.

   The minimum acceptable timeout duration is 30 seconds and the maximum acceptable timeout duration is 43200 seconds. The default timeout duration is 60 seconds.



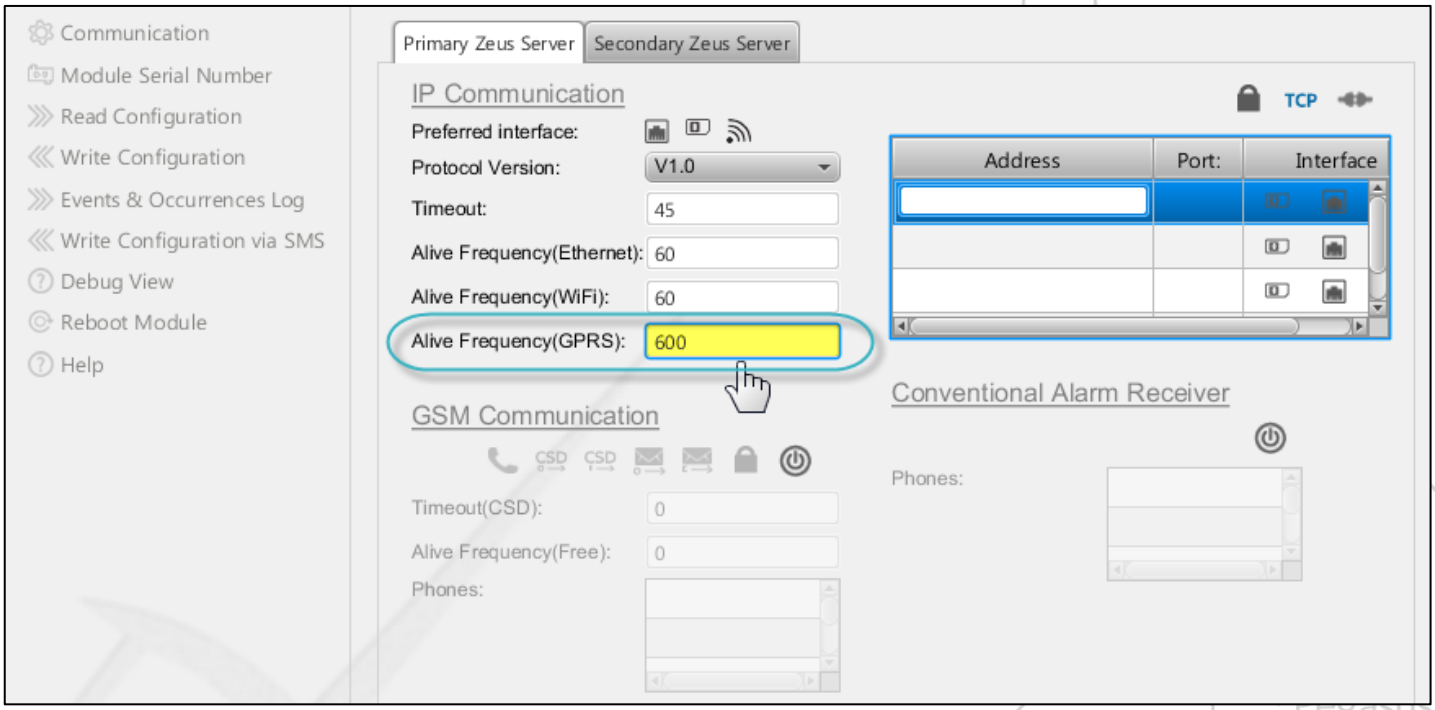
6. In the **Alive Frequency (Wi-Fi)** text box, enter the **Active Frequency of Wi-Fi** in seconds. Here, Pegasus™ NX sends identification/alive packets (Protocol v1.0) or M2S (Protocol v2.0) to the Primary Zeus™ Server via Wi-Fi.

   The minimum acceptable timeout duration is 30 seconds and the maximum acceptable timeout duration is 43200 seconds. The default timeout duration is 60 seconds.

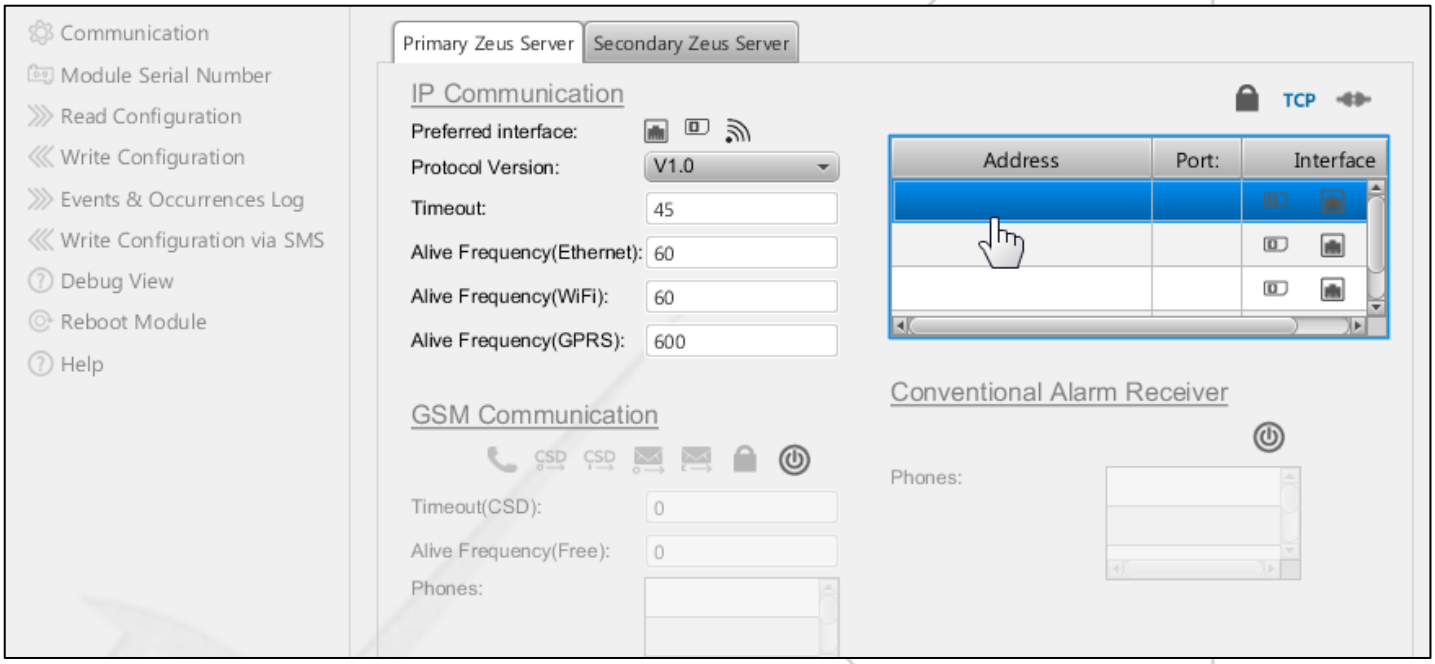


7. In the **Alive Frequency (GPRS)** text box, enter the **Active Frequency of GPRS** in seconds. Here, Pegasus™ NX sends identification/ alive packets (Protocol v1.0) or M2S (Protocol v2.0) to the Primary Zeus™ Server via GPRS.

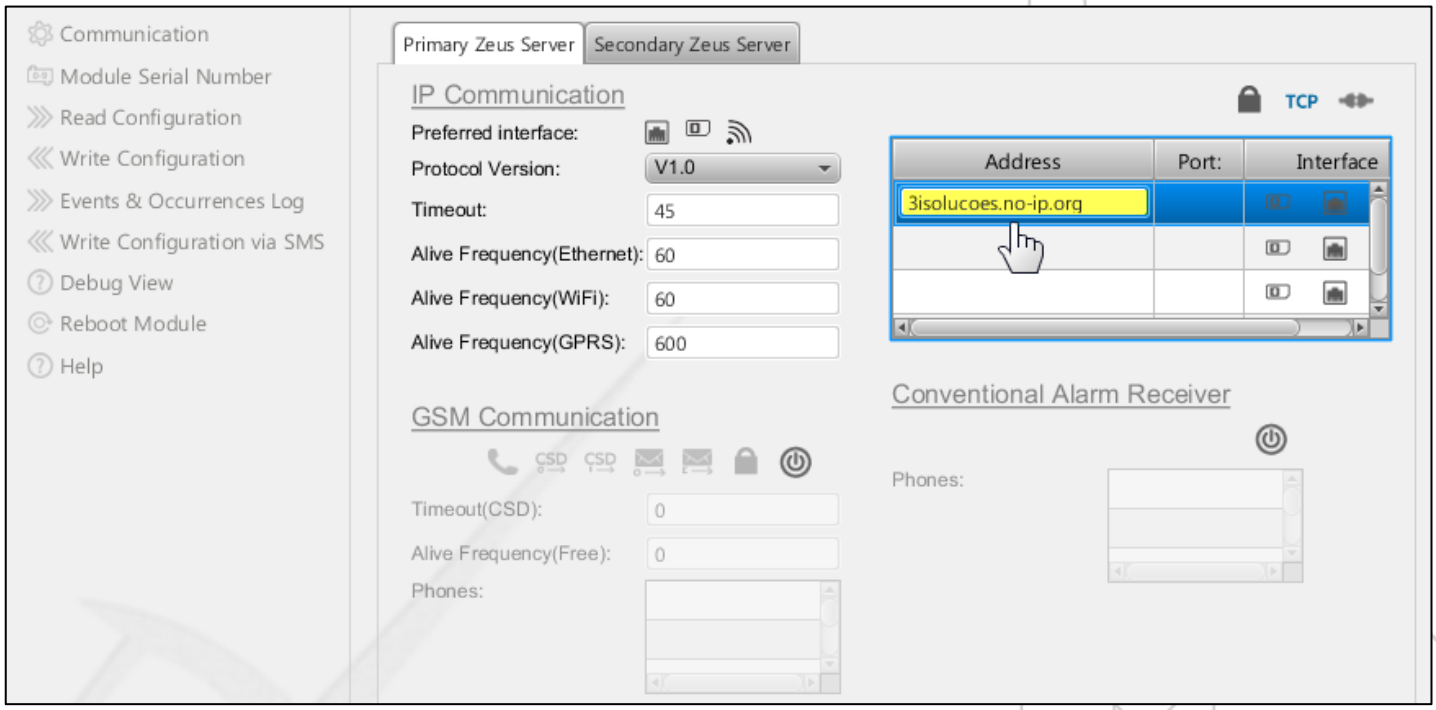
   The minimum acceptable timeout duration is 30 seconds and the maximum acceptable timeout duration is 43200 seconds. The default timeout duration is 60 seconds.



8. Under Address, click to select the 1st row as shown in the below image.

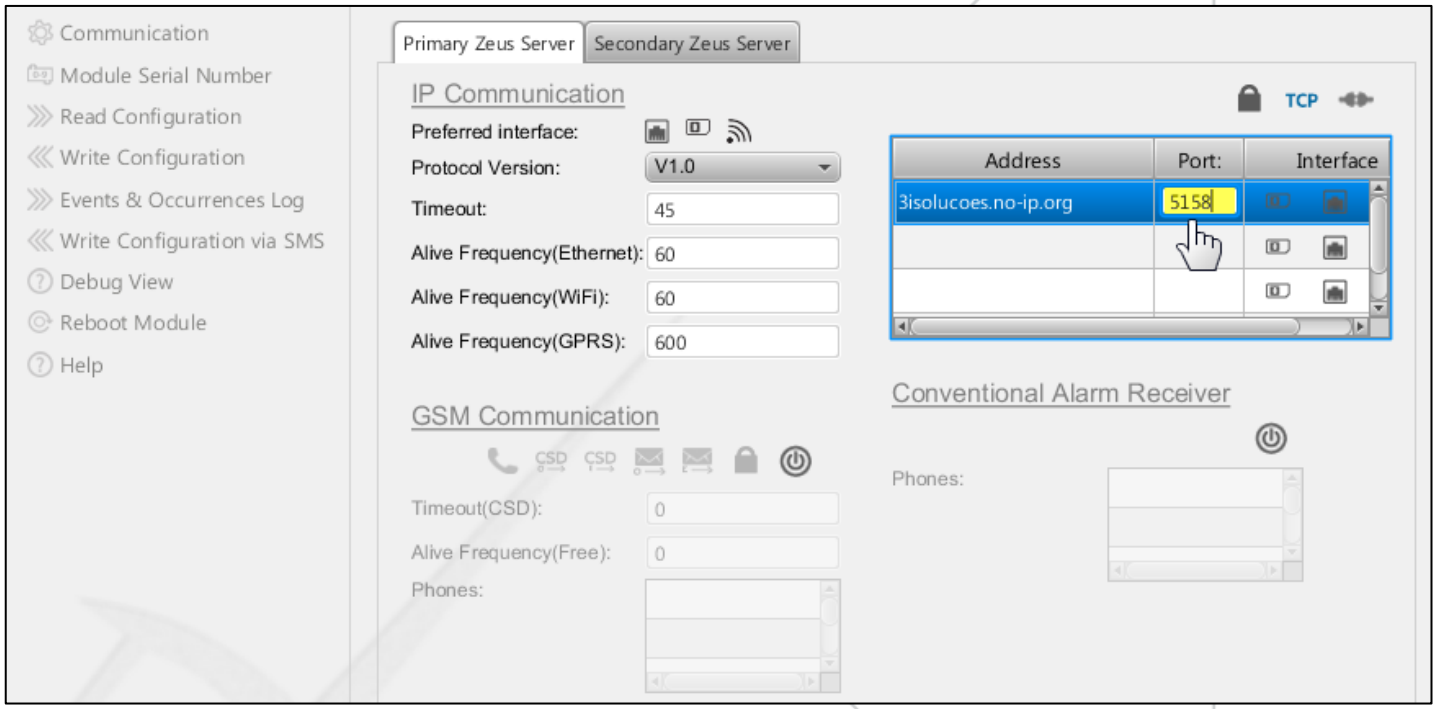


9. Under Address, click-in, and then enter the **URL or IP Address** as shown in the below image.

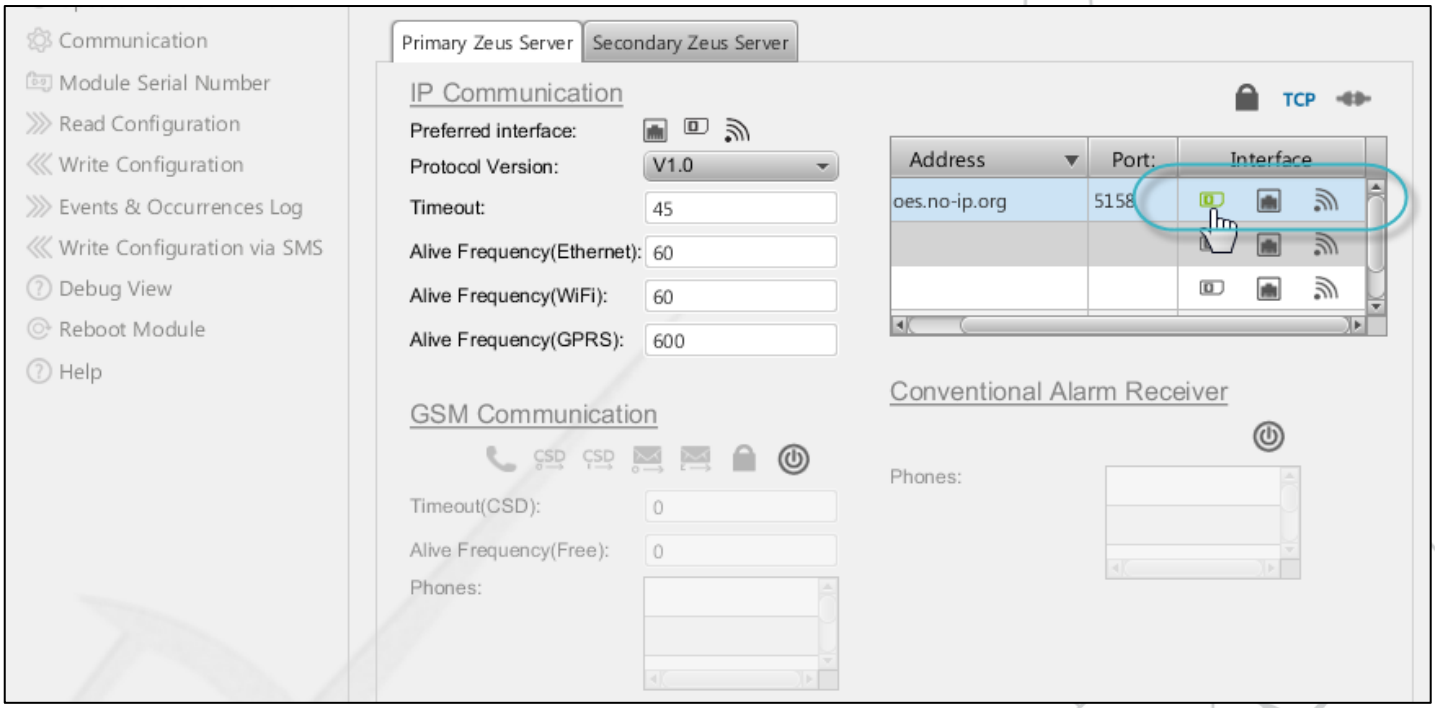


Likewise, you can enter the URL or IP Address in rows: 2, 3, and 4.

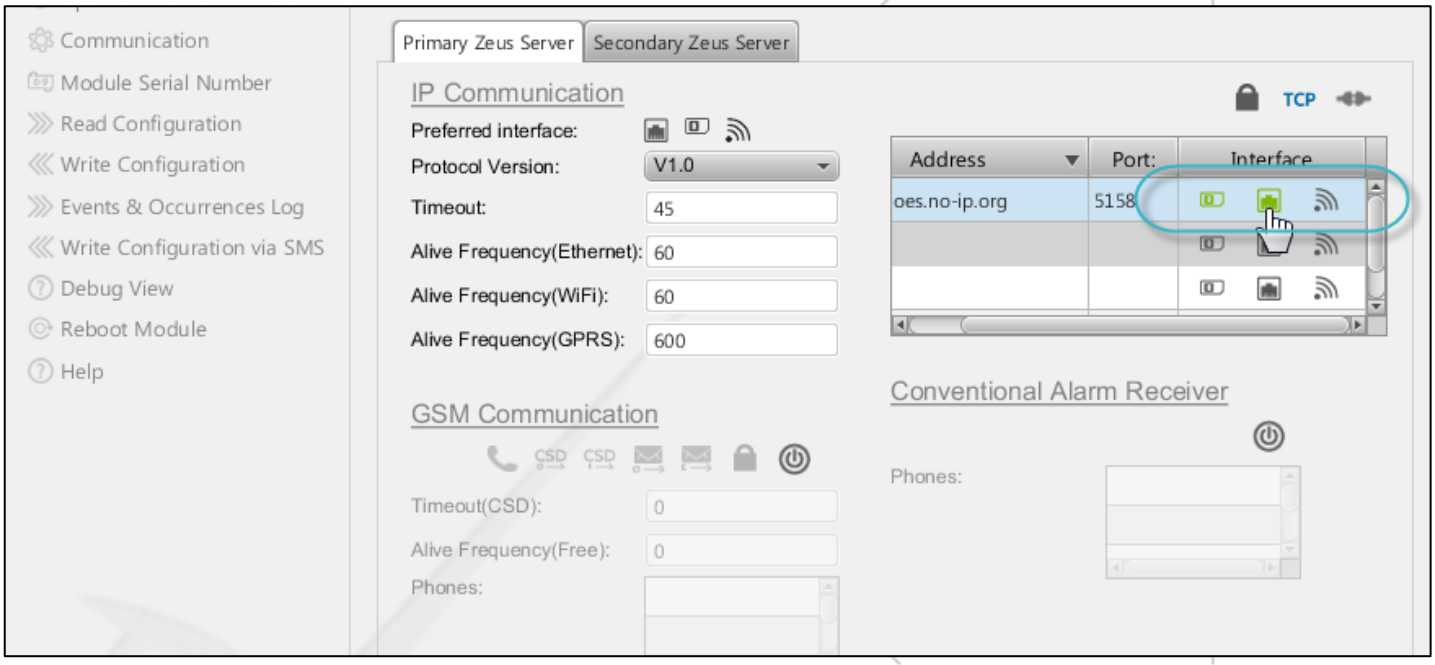
10. Under **Port**, click-in, and then enter the **Port** number adjacent to your URL or IP address as shown in the below image.



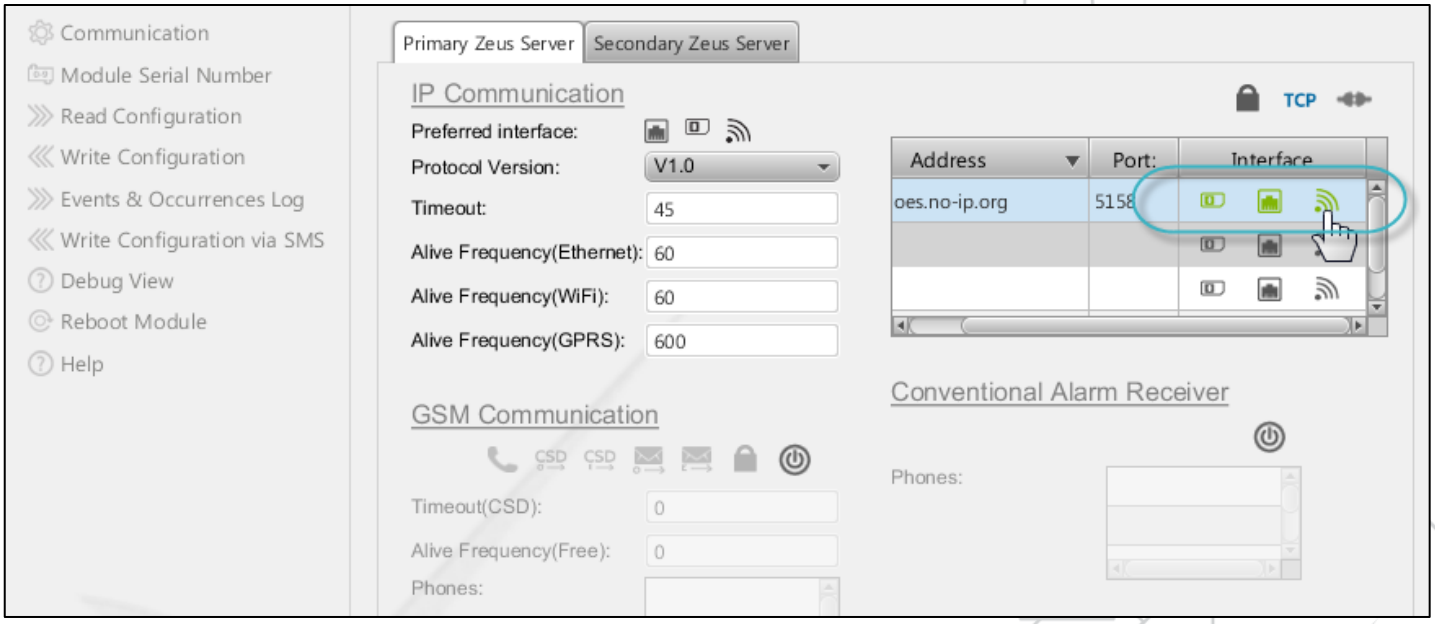
11. Under Interface, to select the GPRS interface, click the inactive **GPRS**  icon. The inactive GPRS icon is turned green  . The **GPRS** interface is selected.



12. Under Interface, to select the Ethernet interface, click the disabled **Ethernet**  icon. The inactive Ethernet icon is turned green  . The **Ethernet** interface is selected.



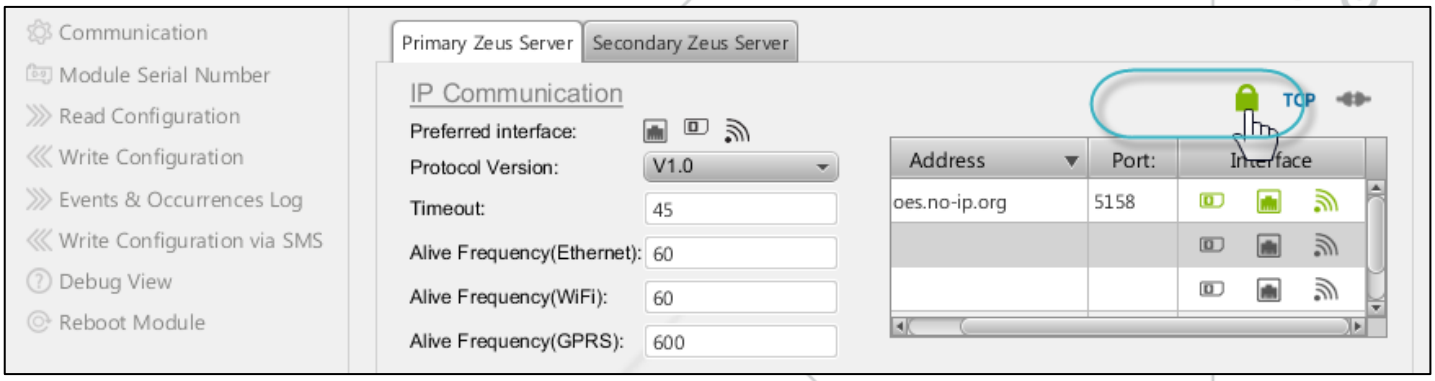
13. Under Interface, to select the Wi-Fi interface, click the disabled **Wi-Fi**  icon. The inactive Wi-Fi icon is turned green  . The **Wi-Fi** interface is selected.



8.2.1.1. Enable Encryption

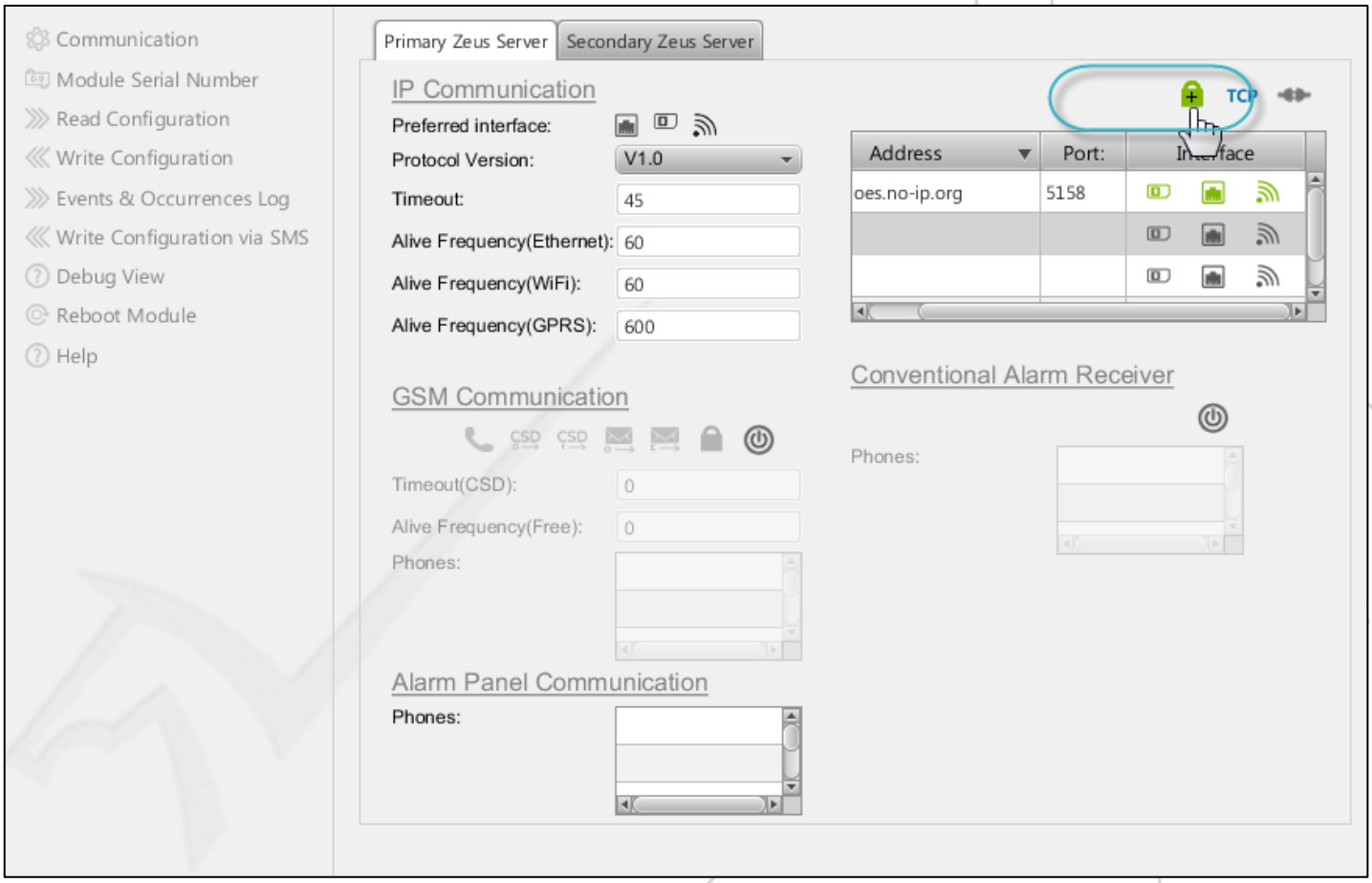
To enable 128-bit encryption

1. Click the grey colored **Encrypt**  icon. The grey colored icon is turned green  as shown in the below image. 128-bit encryption is in the enabled state.



To enable 256-bit encryption

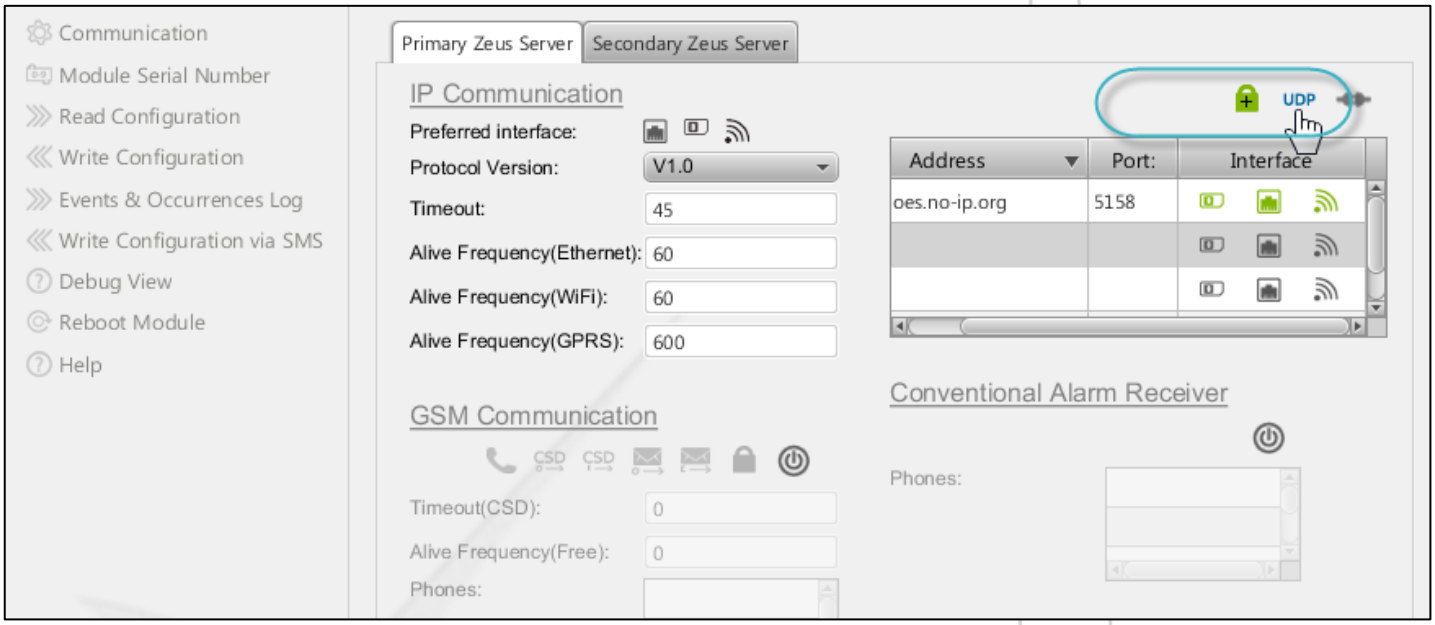
1. Click the green colored **Encrypt 128** icon. A plus sign is displayed on the **Encrypt 128** icon as shown in the below image. 256-bit encryption is in the enabled state.



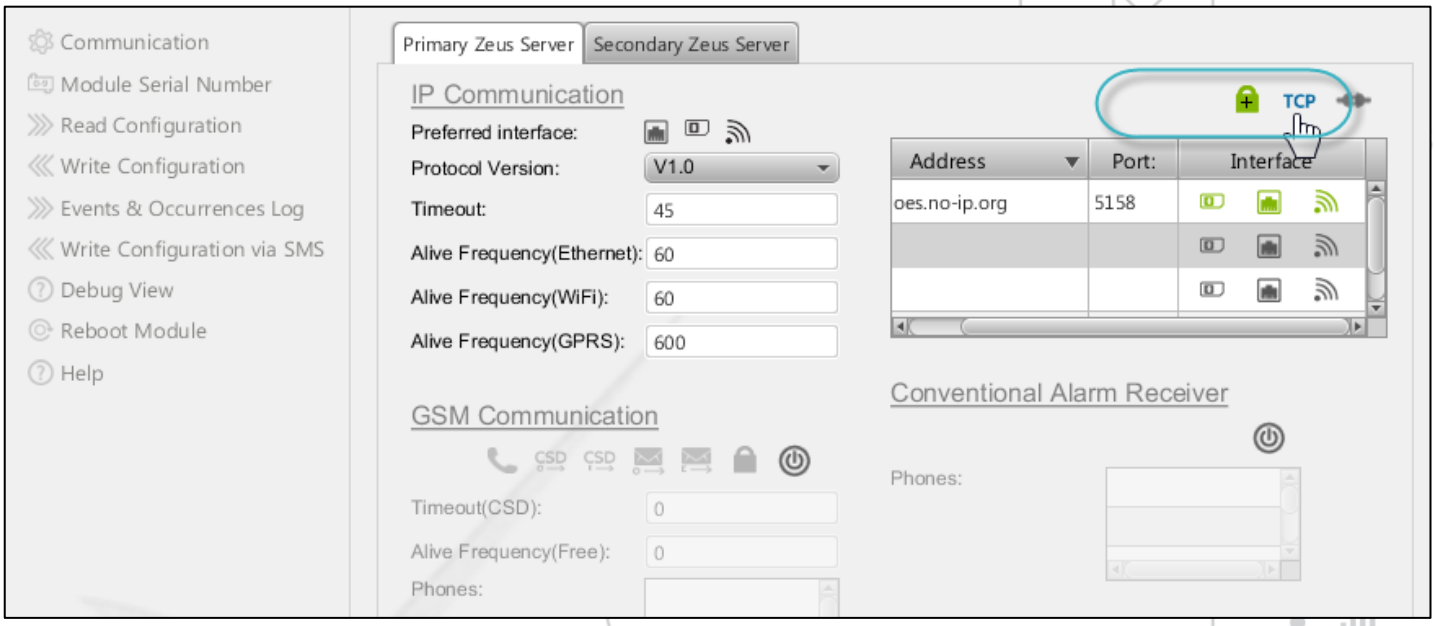
8.2.1.2. Enable TCP/UDP

To enable network protocol: TCP

1. Click the **UDP** icon.

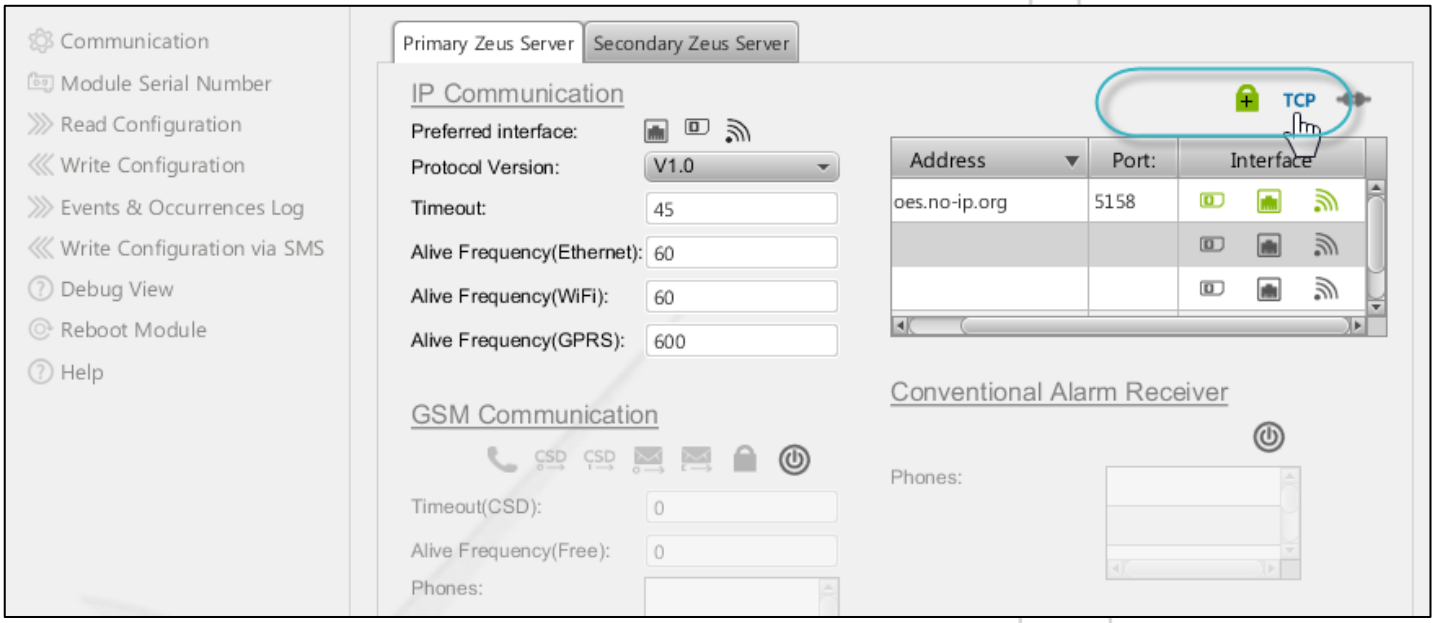


The UDP  icon is changed as the TCP  icon as shown in the below image. **Network protocol: TCP** is in the enabled state.

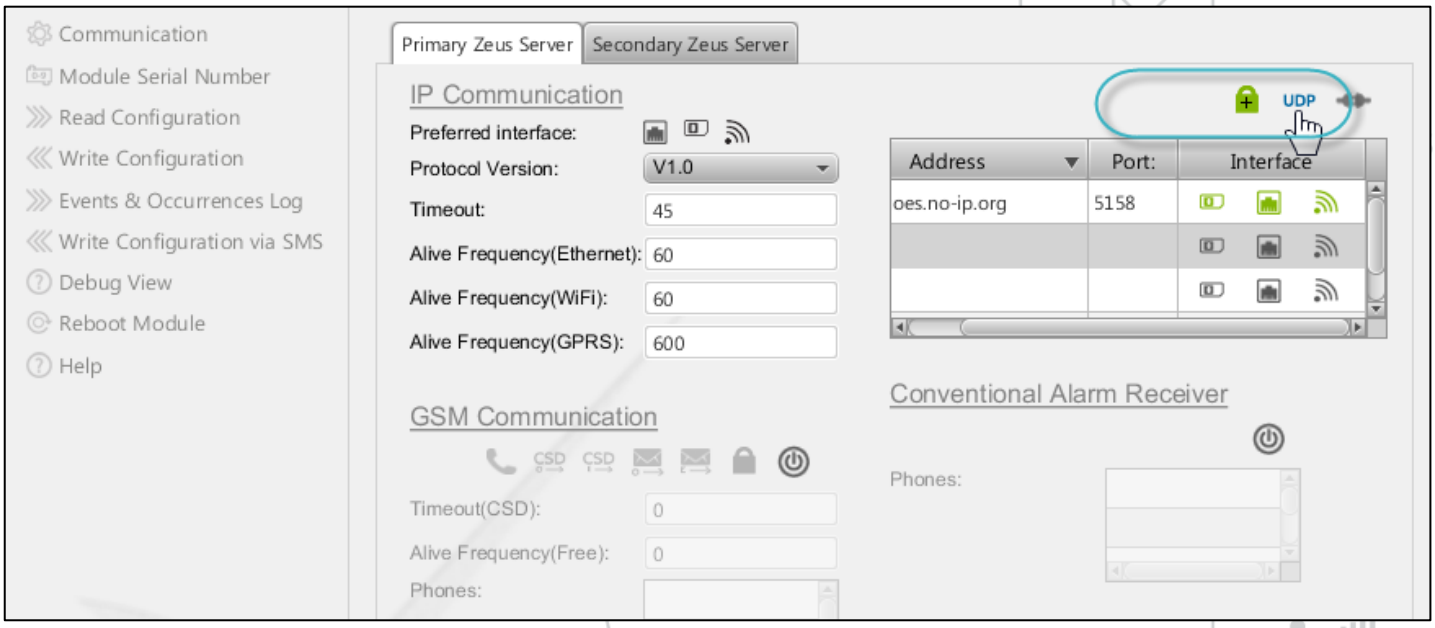


To enable network protocol: UDP

1. Click the **TCP**  icon.



The TCP  icon is changed as the UDP  icon as shown in the below image. **Network protocol: UDP** is in the enabled state.

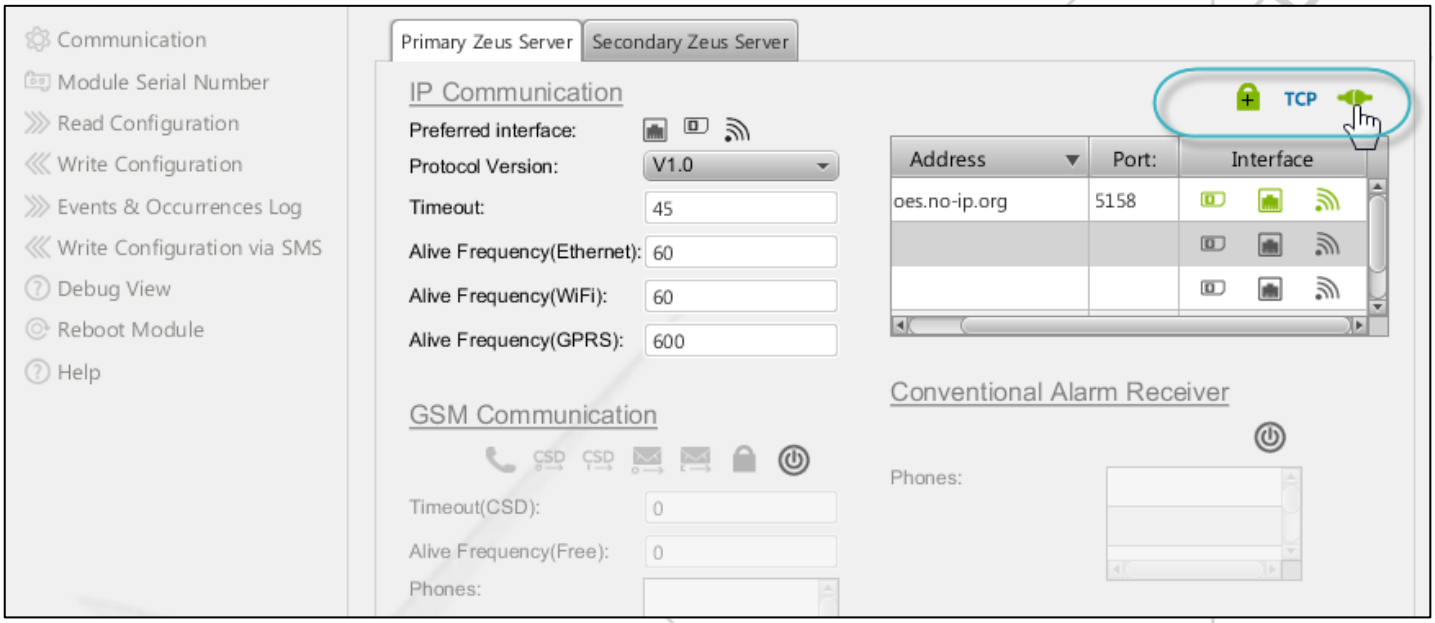


8.2.1.3. Enable Persistent Connection

To enable persistent connection

1. Click the grey colored **Enable Persistent Connection**  icon as shown in the below image.

The grey colored icon is turned green  as shown in the below image. **Persistent connection** is in the enabled state.

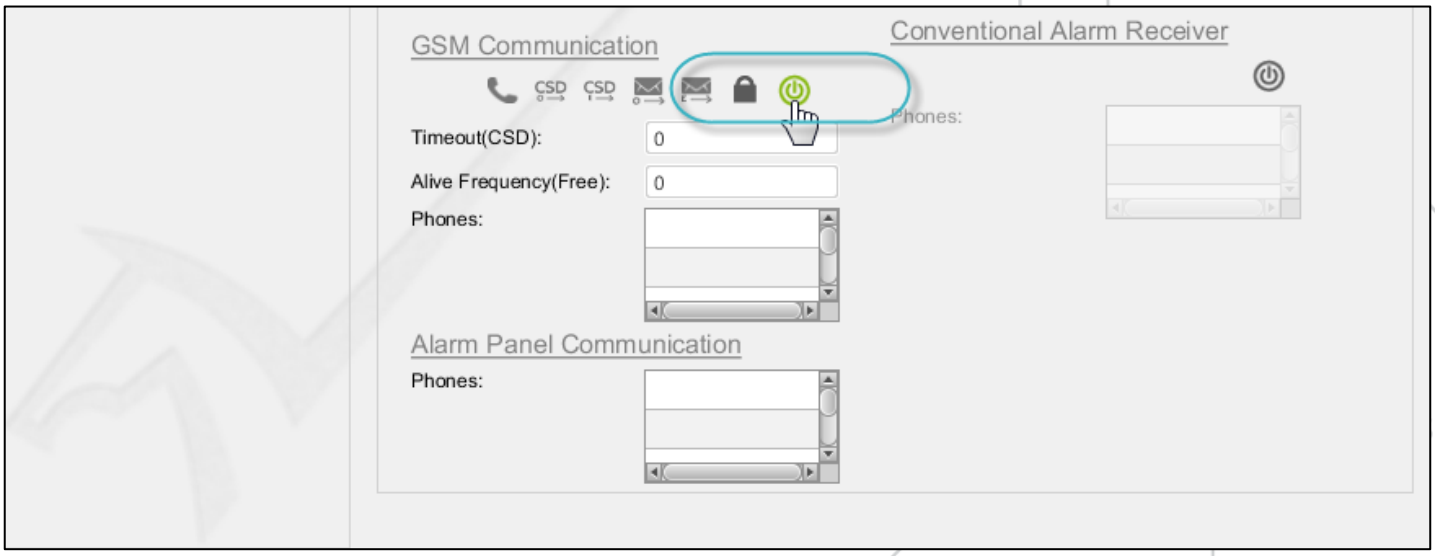


8.2.2. Configure GSM Communication

8.2.2.1. Enable GSM Communication

To enable gsm communication

1. Click the grey colored **Enable GSM Communication**  icon. The grey colored icon is turned green  as shown in the below image. **GSM Communication** is in the enabled state.



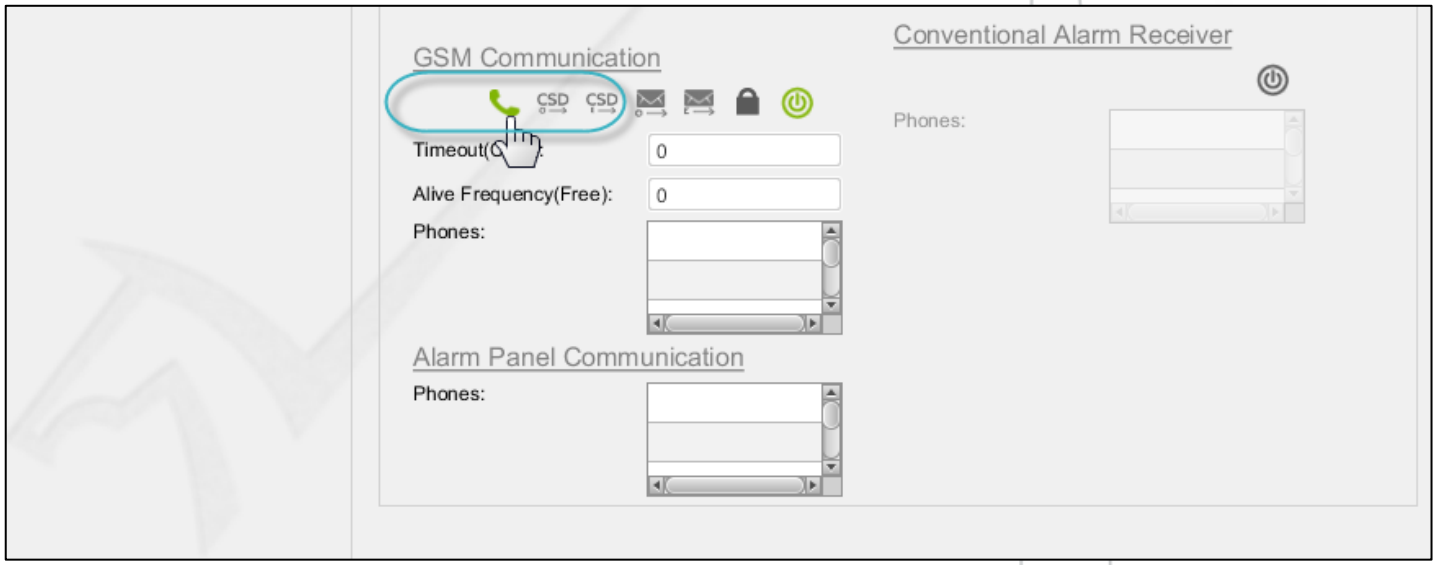
8.2.2.2. Enable Send Alive Packets via Free Call

This feature permits sending of alive packets via free call, and is available only when the GSM communication is in the enabled state.

To enable send alive packets via free call

1. Click the **Send Alive Packets via Free Call**  icon. The grey colored icon is turned green  as shown in the below image.

   The **Send Alive Packets via Free Call** feature is in the enabled state.



8.2.2.3. Enable Send Occurrence Packets via CSD

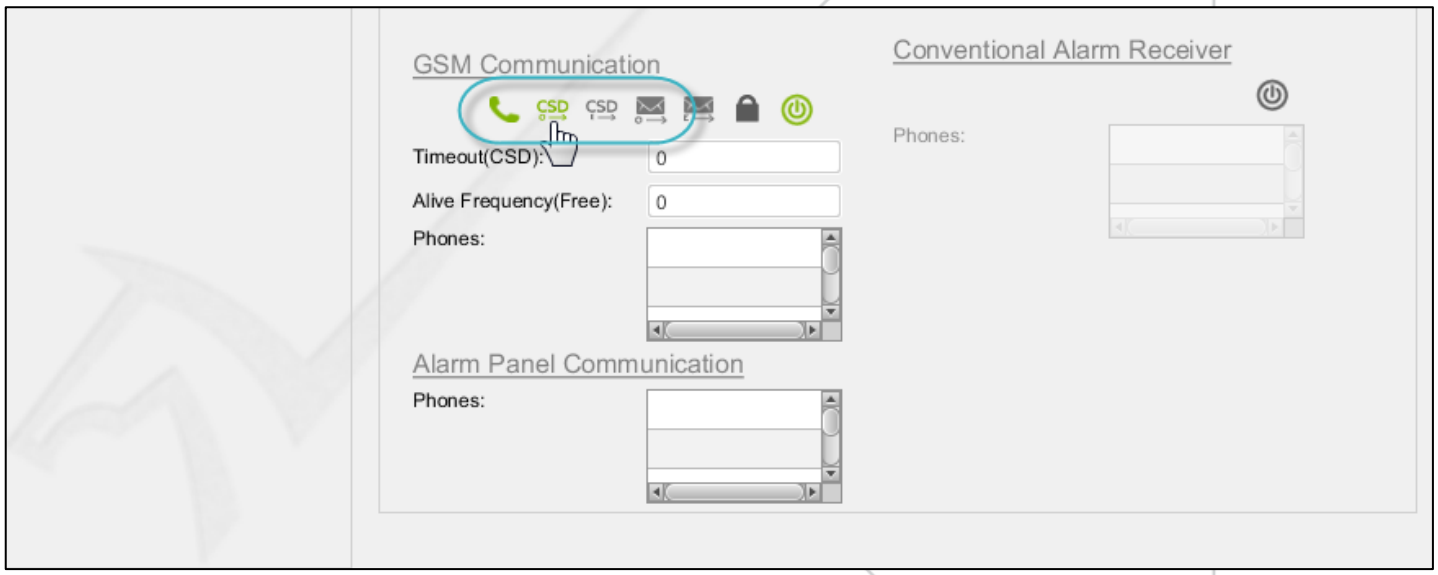
This feature permits sending of occurrence packets via CSD, and is available only when the GSM communication is the enabled state.

To send occurrence packets via csd

1. Click the **Send Occurrence Packets via CSD** 

icon. The grey colored icon is turned green 

as shown in the below image. The **Send Occurrence Packets via CSD** feature is in the enabled state.

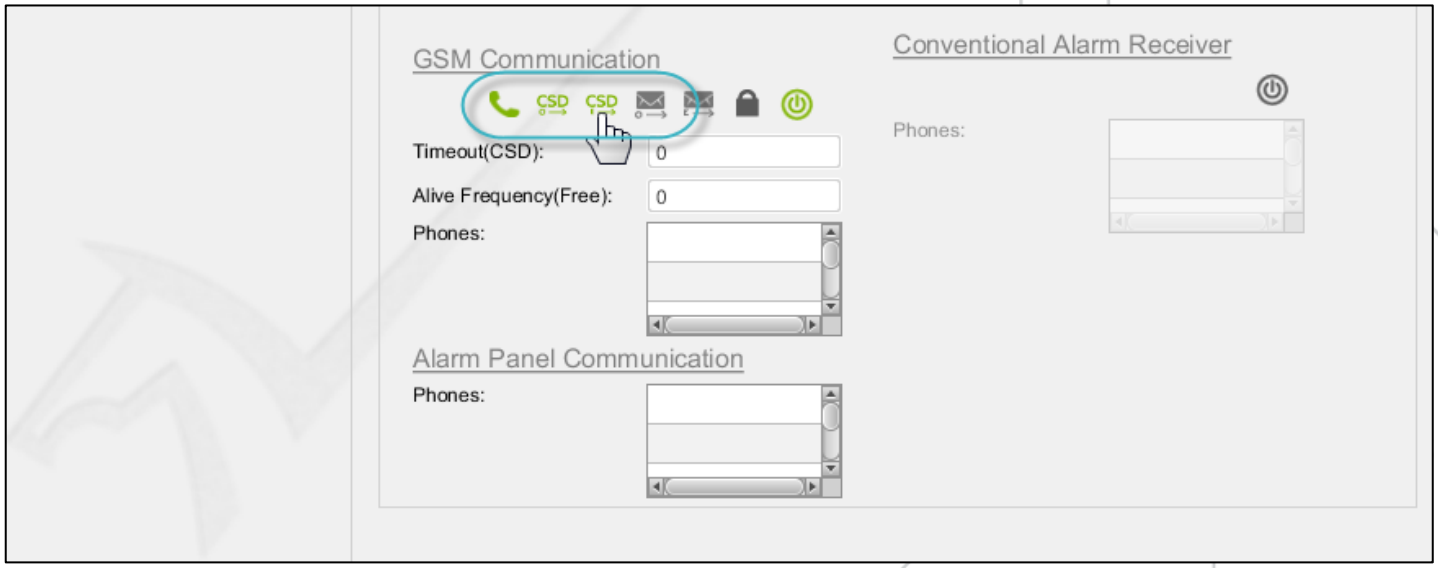


8.2.2.4. Enable Send Event Packets via CSD

This feature permits sending of event packets via CSD, and is available only when the GSM communication is the enabled state.

To enable send event packets via csd

1. Click the **Send Event Packets via CSD**  icon. The grey colored icon is turned green  as shown in the below image. The **Send Event Packets via CSD** feature is in the enabled state.



Note:

If Send Occurrence Packets via CSD and Send Event Packets via CSD are in the enabled state, the following features are in the inactive state:

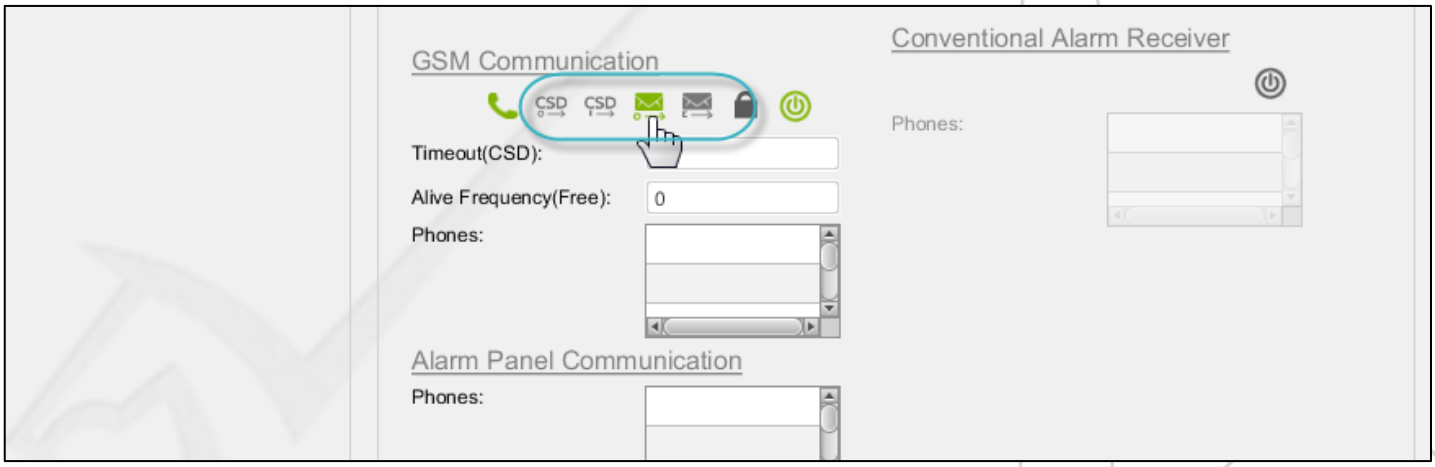
- Send Occurrence Packets via SMS
- Send Event Packets via SMS

8.2.2.5. Enable Send Occurrence Packets via SMS

This feature permits sending of occurrence packets via SMS, and is available only when the GSM communication is the enabled state.

To enable send occurrence packets via sms

1. Click the **Send Occurrence Packets via SMS** icon. The grey colored icon is turned green as shown in the below image. The **Send Occurrence Packets via SMS** feature is in the enabled state.

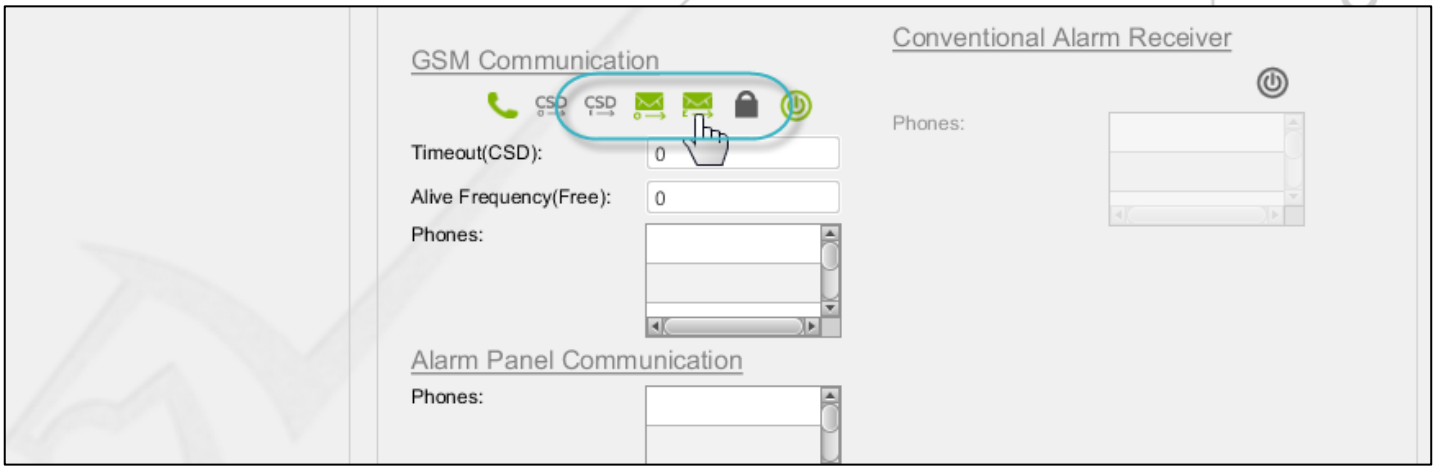


8.2.2.6. Enable Send Event Packets via SMS

This feature permits sending of event packets via SMS, and is available only when the GSM communication is the enabled state.

To enable send event packets via sms

1. Click the **Send Event Packets via SMS** icon. The grey colored icon is turned green as shown in the below image. The **Send Event Packets via SMS** feature is now in the enabled state.



Note:

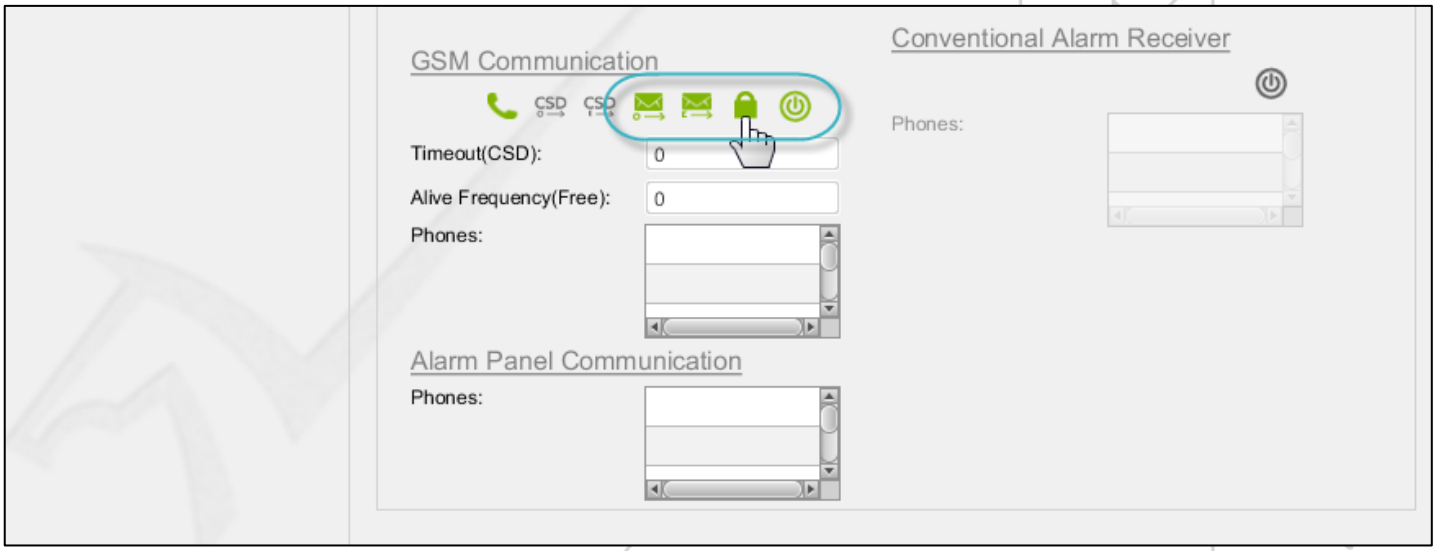
If Send Occurrence Packets via SMS and Send Event Packets via SMS are in the enabled state, the following features are in the inactive state:

- Send Occurrence Packets via CSD
- Send Event Packets via CSD

8.2.2.7. Enable 128/256-Bit Encryption

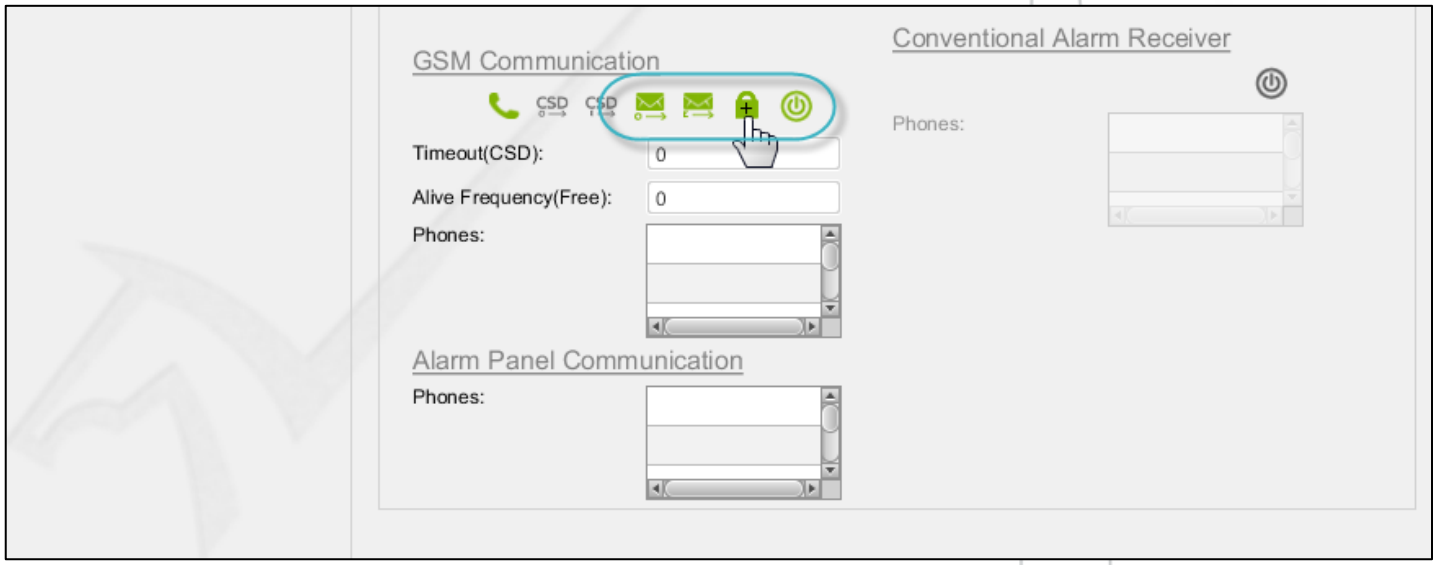
To enable 128-bit encryption

1. Click the grey colored **Encrypt**  icon. The grey colored icon is turned green  as shown in the below image. 128-bit encryption is in the enabled state.



To enable 256-bit encryption

2. Click the green colored **Encrypt 128**  icon. A plus sign is displayed on the **Encrypt 128**  icon as shown in the below image. 256-bit encryption is in the enabled state.

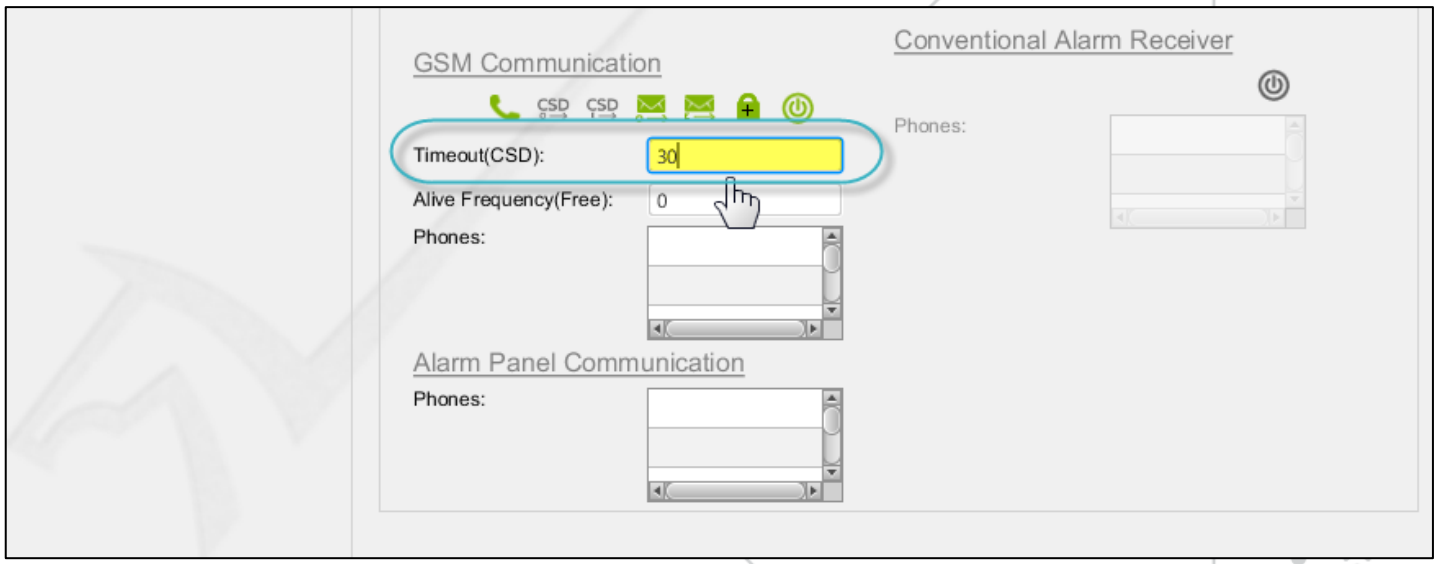


8.2.2.8. Configure GSM Communication

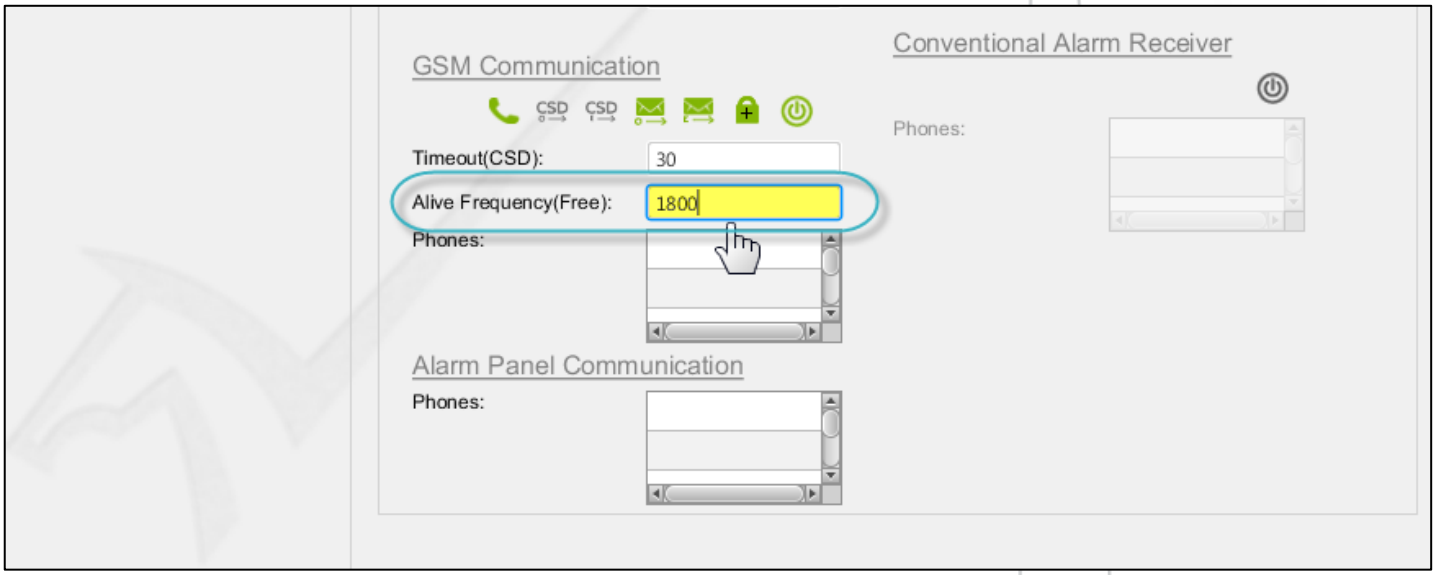
To configure gsm communication

1. In the **Timeout(CSD)** text box, type-in the GSM communication timeout duration in seconds.

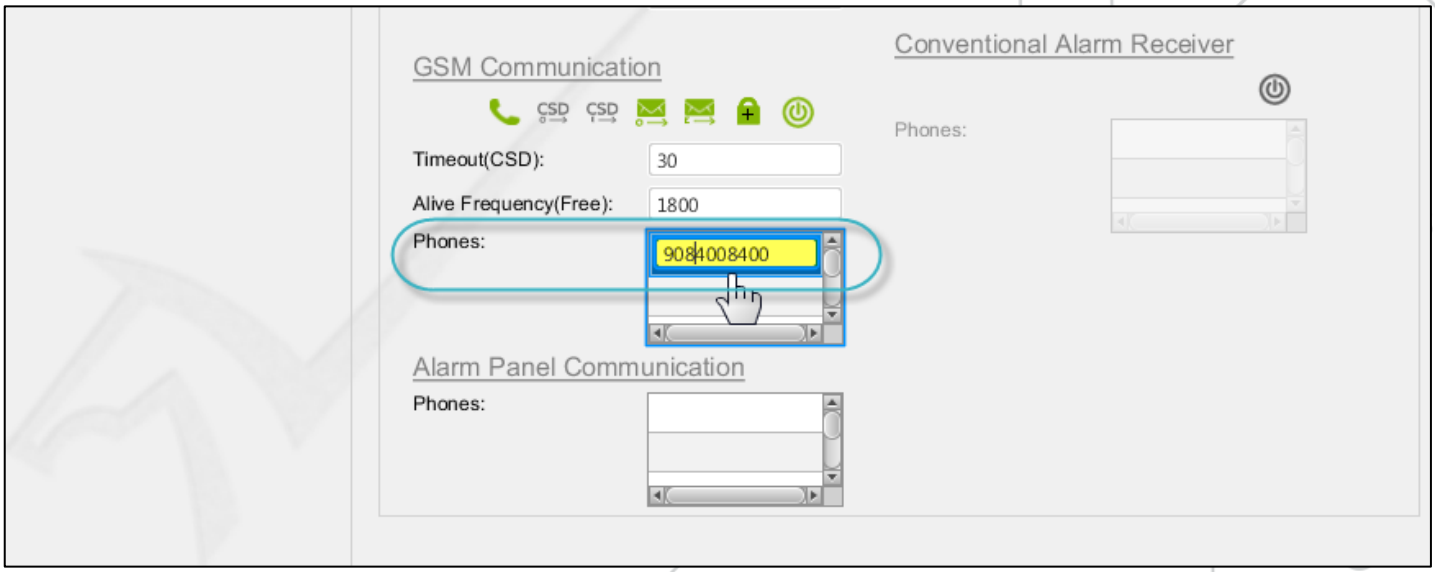
   The minimum acceptable duration is 15 seconds and the maximum acceptable duration is 180 seconds. The default timeout duration is 30 seconds.



2. In the **Alive Frequency(Free)** text box, enter the alive frequency of free call in seconds. The minimum acceptable duration is 60 seconds and the maximum acceptable duration is 3600 seconds. The default duration is 1800 seconds.



3. In the **Phones** scroll box, double-click a row and then type-in the phone number as shown in the below image. The **Phones** scroll box is built-in four rows in which four phone numbers can be configured.



Likewise, you can enter phone numbers in other rows.

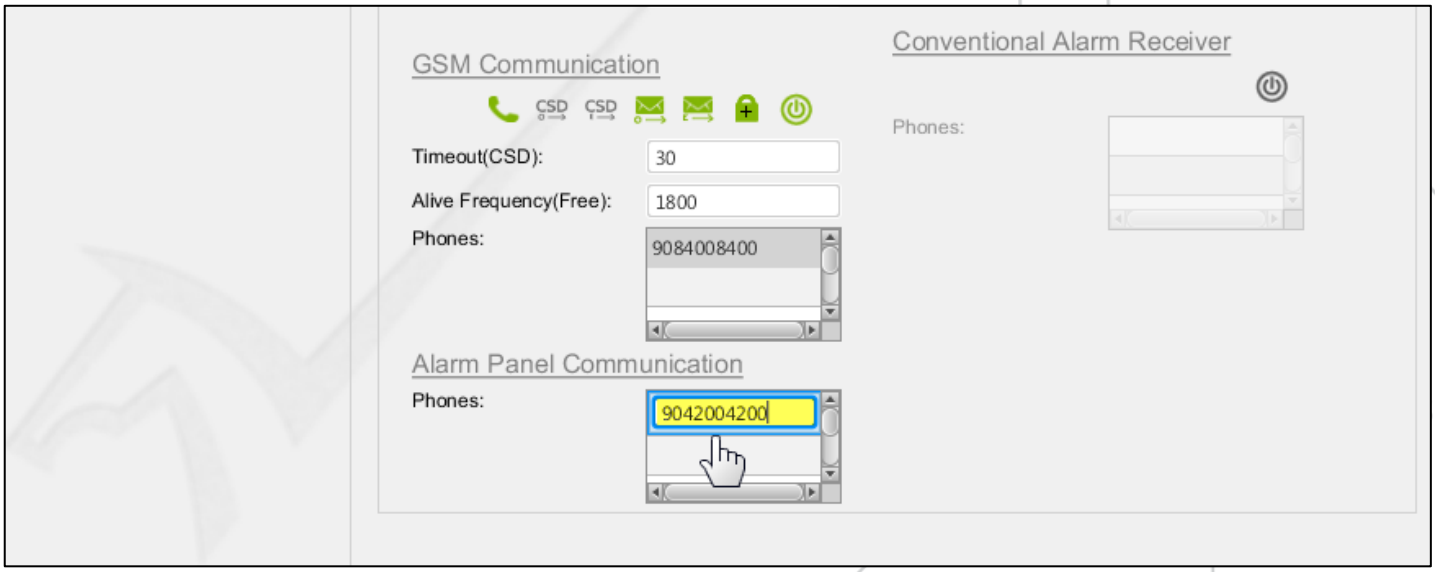
8.2.3. Configure Alarm Panel Communication

8.2.3.1. Configure Phone Numbers

Under Alarm Panel Communication, in the **Phones** scroll box, upto four phone numbers can be configured. The configured phone numbers are used for the alarm panel communication.

To configure phone numbers

1. In the **Phones** scroll box, double-click a row and then type-in the phone number as shown in the below image.



Likewise, you can enter phone numbers in other rows.

8.2.4. Configure Conventional Alarm Receiver

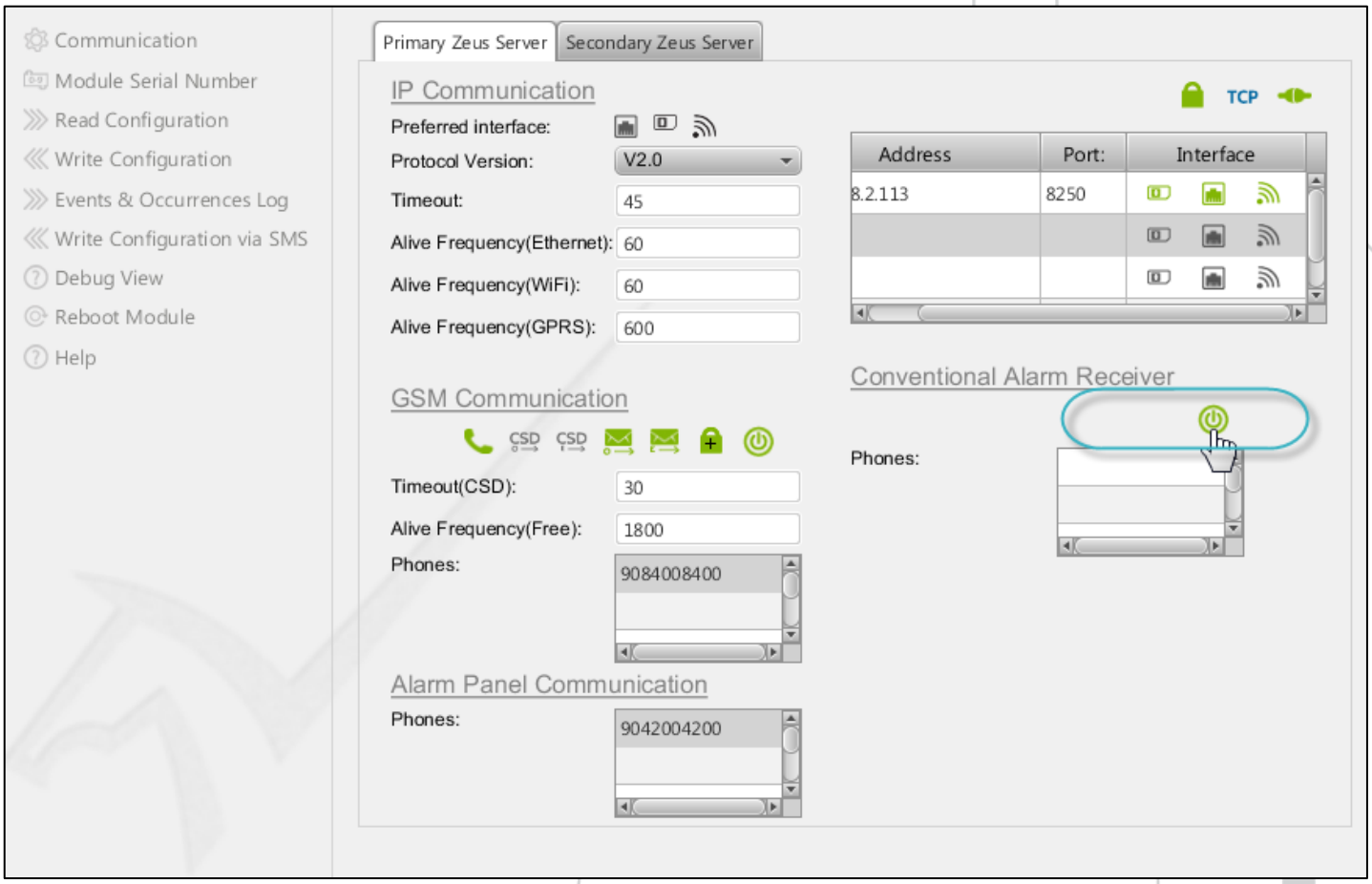
In Pegaus™ NX, if all communication options fails, communication with the Zeus™ Server is still possible via Conventional Alarm Receiver which becomes active after your preferred interface: Ethernet, Wi-Fi and GPRS fails for three times.

If free call, csd or sms is enabled, the Conventional Alarm Receiver will only work if any of the gsm communication options: free call, csd or sms fails.

8.2.4.1. Enable Conventional Alarm Receiver

To enable conventional alarm receiver

1. To enable the conventional alarm receiver, click the grey colored **Enable Conventional Alarm Receiver** icon. The grey colored icon is turned green as shown in the below image. The **Conventional Alarm Receiver** is in the enabled state.



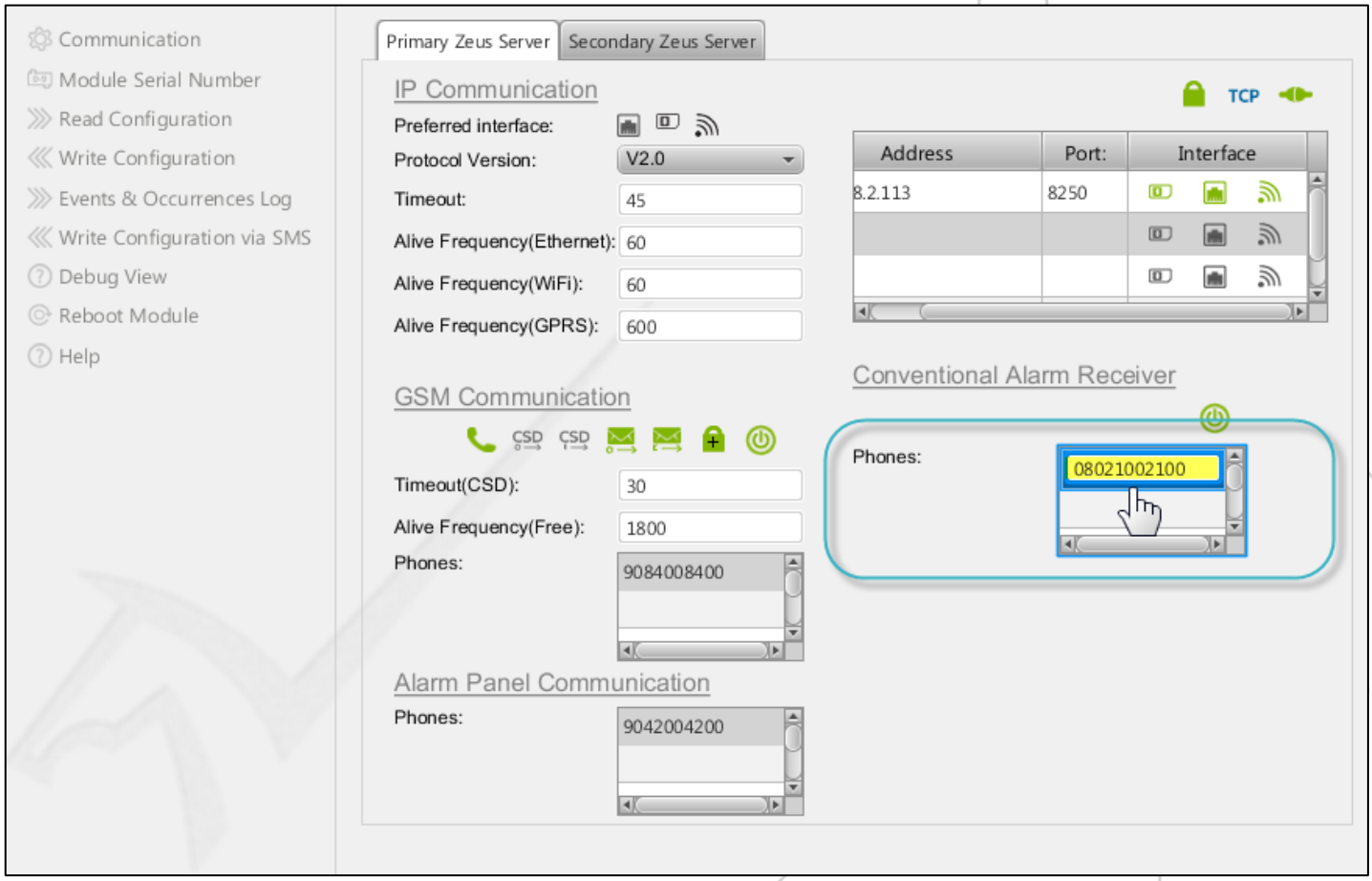
8.2.4.2. Configure Conventional Alarm Receiver

Once the Conventional Alarm Receiver is enabled, configure phone numbers in the **Phones** scroll box. Total four phone numbers can be configured.

The configured phone numbers are used for the conventional alarm receiver communication.

To configure conventional alarm receiver

1. In the **Phones** scroll box, double-click a row, and then type-in the phone number of the handset which is connected to the conventional alarm receiver.

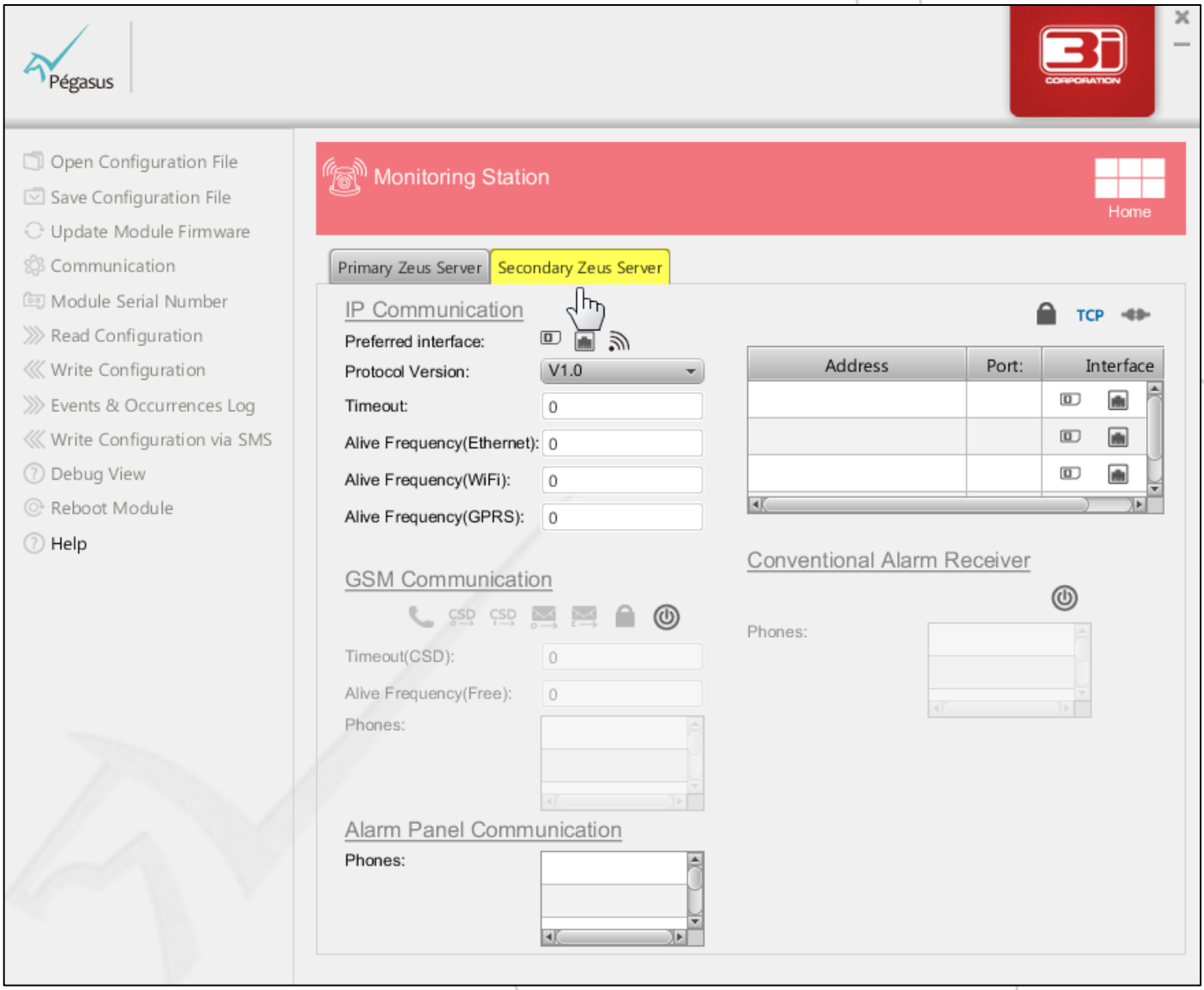


Likewise, you can enter phone numbers in other rows.

8.3. Configure Secondary Zeus™ Server

To configure the secondary Zeus™ server

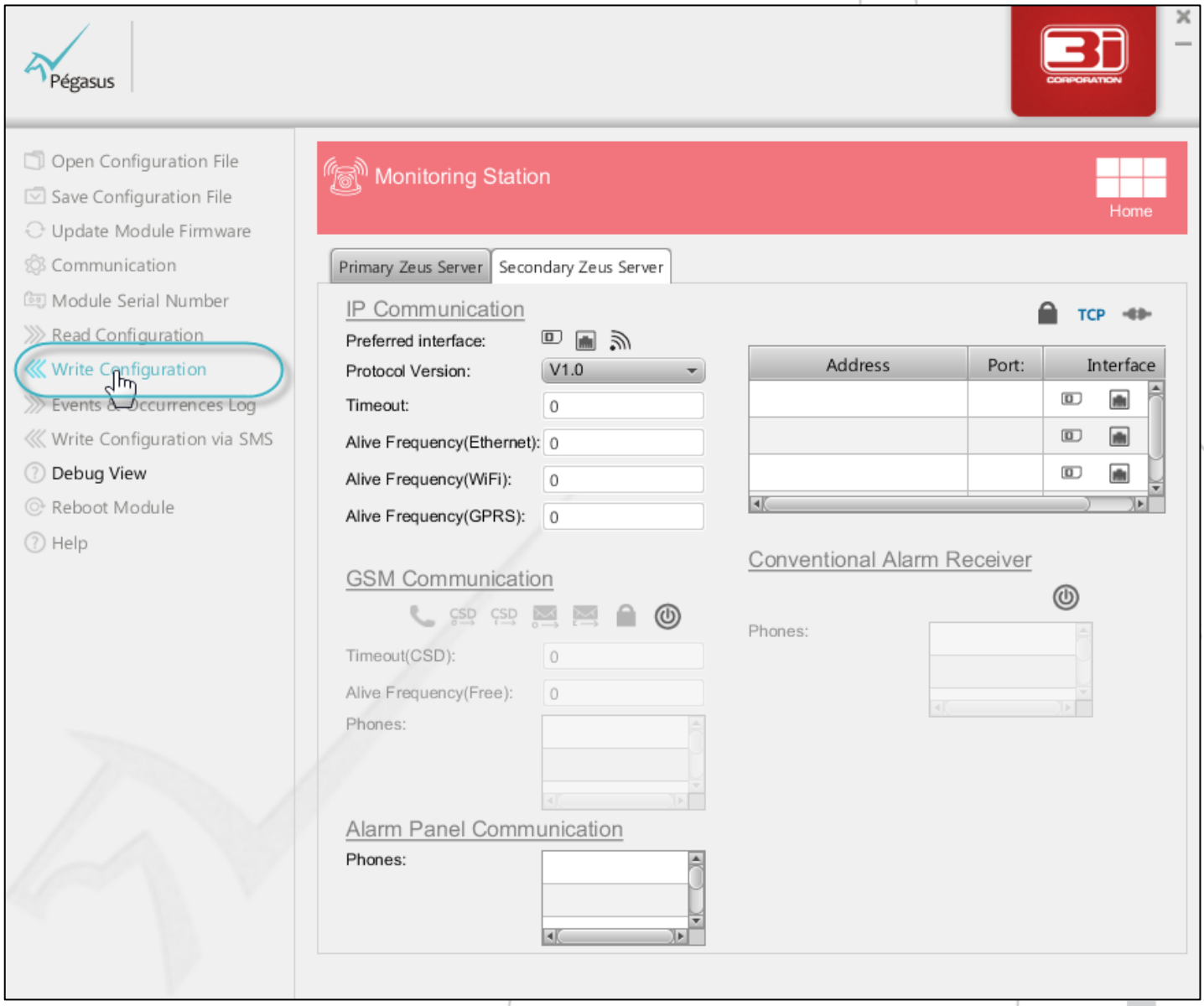
1. Click the **Secondary Zeus™ Server** tab. The **Secondary Zeus™ Server** interface is displayed.



2. The Secondary Zeus™ Server configuration is similar to the Primary Zeus™ Server. To configure the Secondary Zeus™ Server, refer step **8.2: Configure Primary Zeus™ Server**.

8.4. Write Configuration

When the Monitoring Station configuration is done, write configuration settings to Pegasus™ NX.

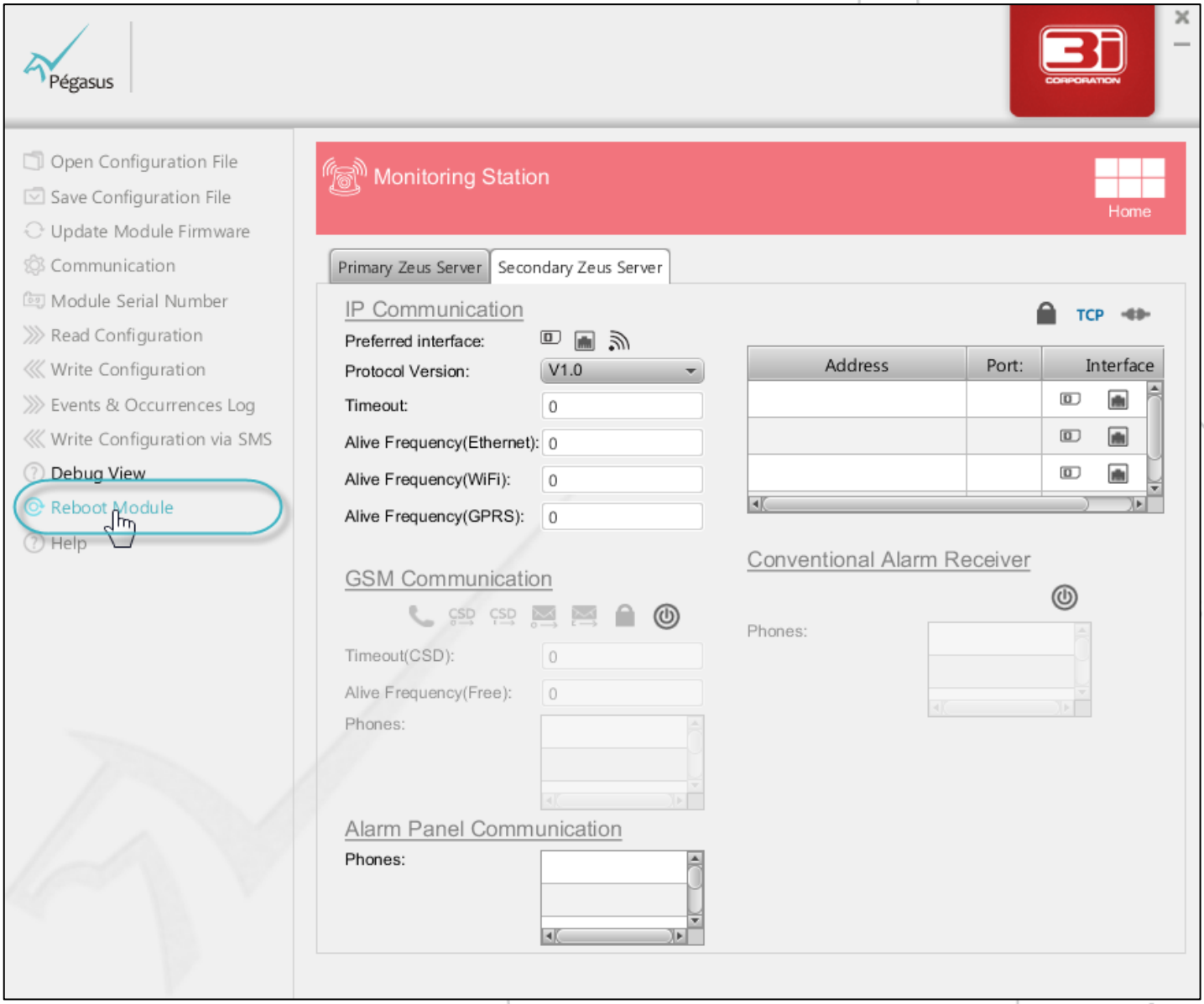


Note:

To learn how to write the configuration settings to Pegasus NX, refer the **Write Configuration** chapter.

8.5. Reboot Module

On successful writing of the Pegasus NX configfuration settings, to make all configured features functional, reboot of module is required.



Note:

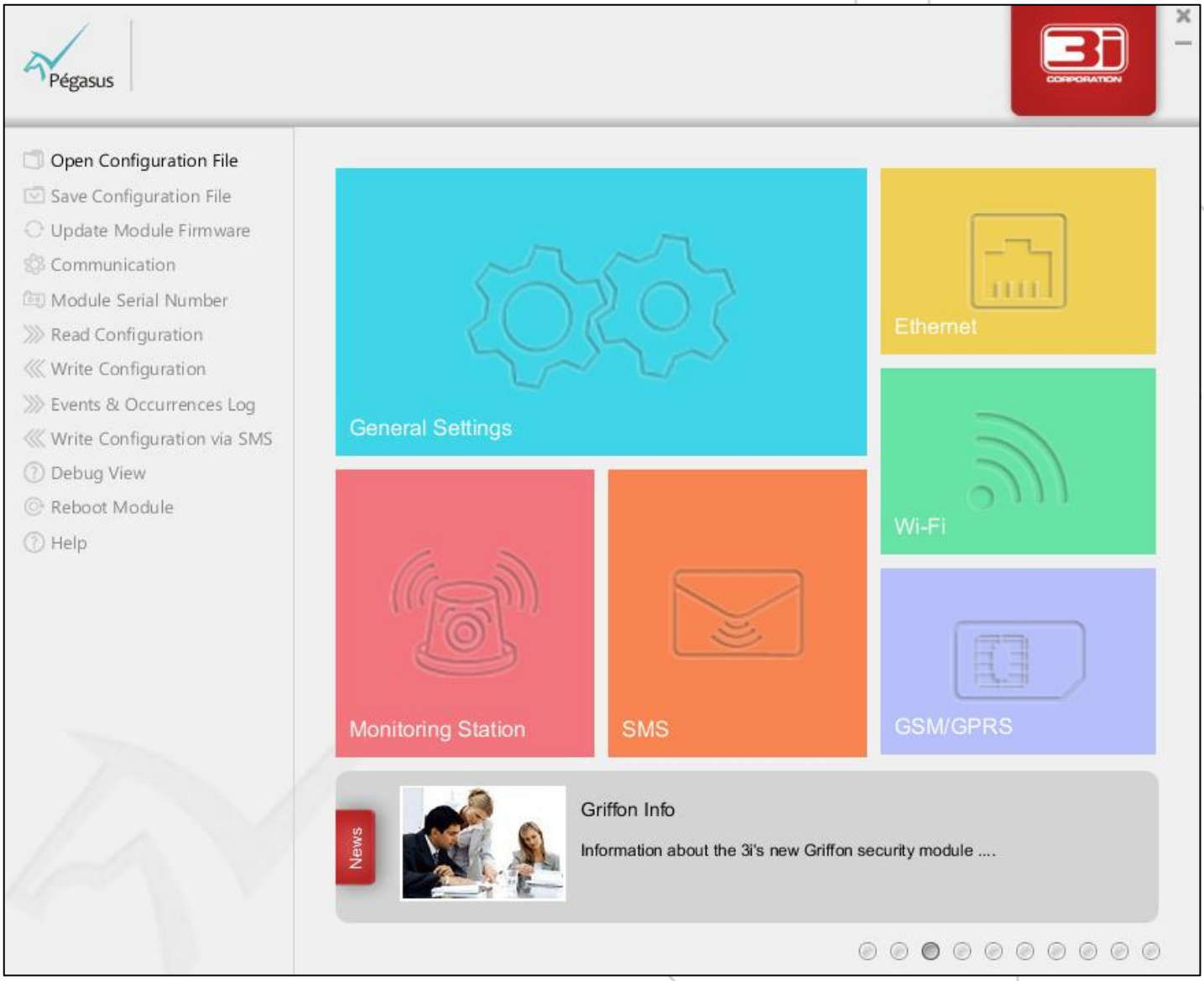
To learn how to reboot module after writing the configuration to Pegasus™ NX, refer the **Reboot Module** chapter.

8.6. Return Back to the Home Screen

To return back to the home screen

1. Click the **Home** icon as shown in the below image.

The **Pegasus™ Studio Home Screen** is displayed.



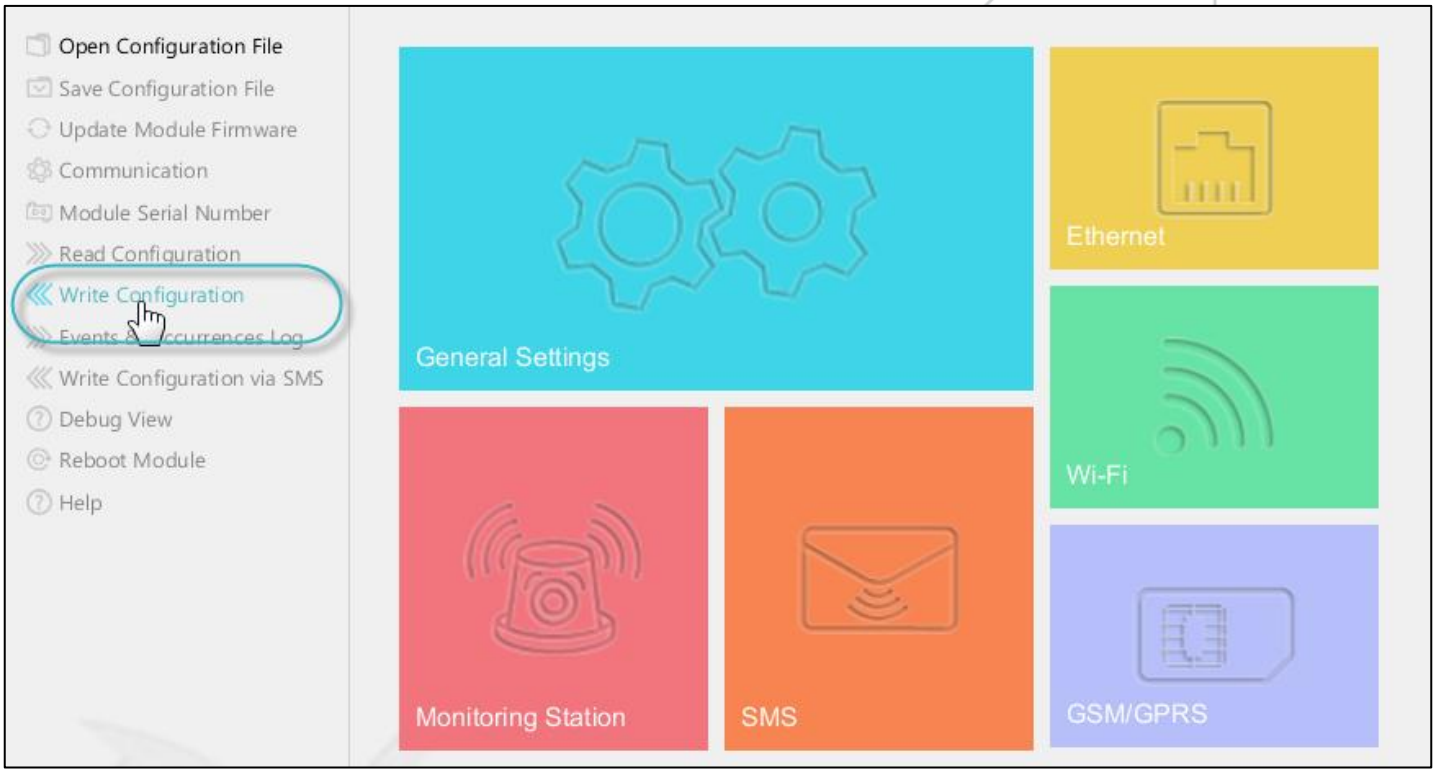
9 Write Configuration

The **Write Configuration** feature allows you to write the configuration settings to Pegasus™ NX. Once the configuration is written to the device, it is stored in its flash memory.

9.1. Write the Configuration Settings to Pegasus™ NX

To write the configuration settings to Pegasus™ NX

1. Open the **Pegasus™ Studio Main Screen,** and then click **Write Configuration.**



A message box saying, “Do you want to send the current configuration to the module?” is displayed.

2. Click the **Yes** button.

A message box saying, “Send configuration successfully completed” is displayed.

3. To close the message box, click the **OK** button.

Note:

To learn how to reboot module after writing the configuration to your Pegasus™ Module, refer the **Reboot Module** chapter.

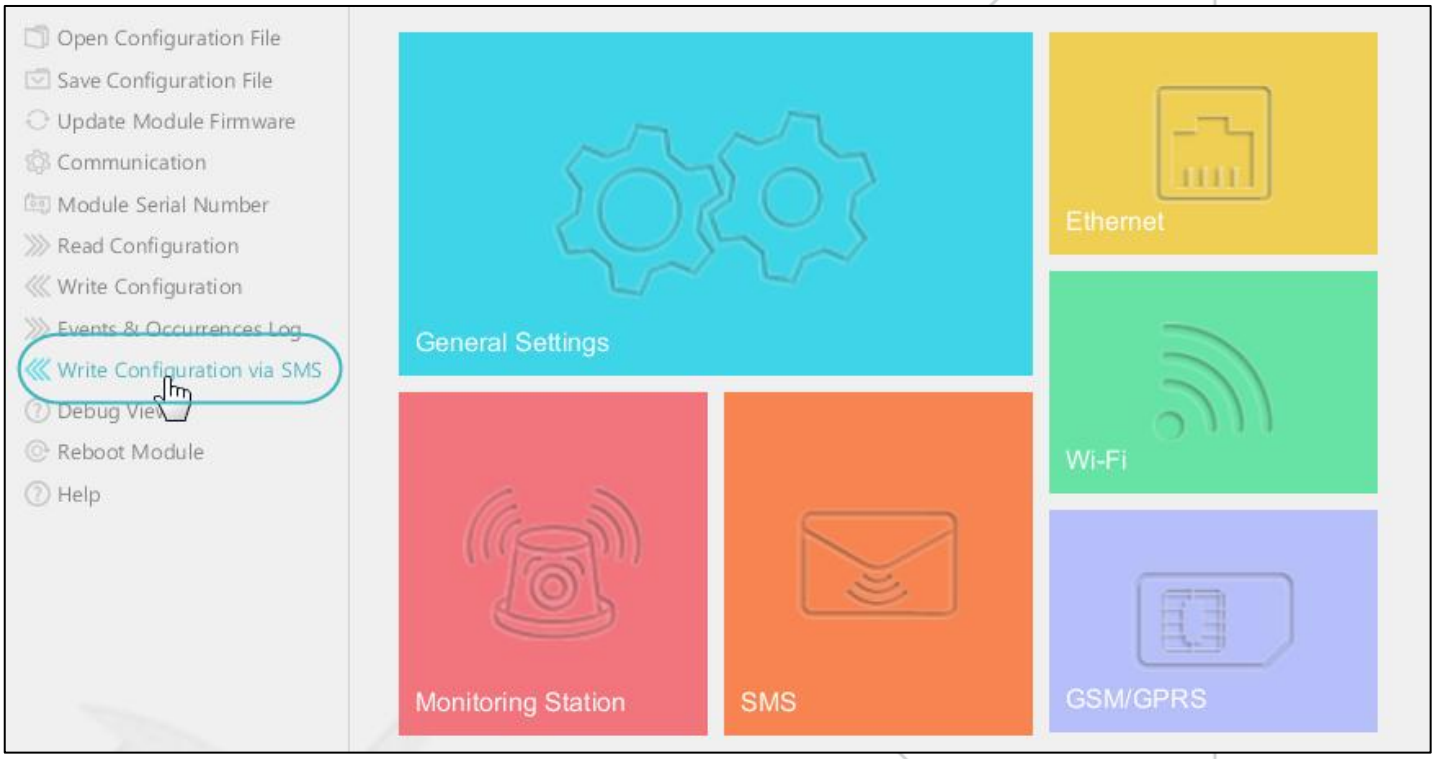
10 Write Configuration via SMS

The **Write Configuration via SMS** feature allows you to write the configuration settings to Pegasus™ NX via SMS. Once the configuration is written to the device, it is stored in its flash memory.

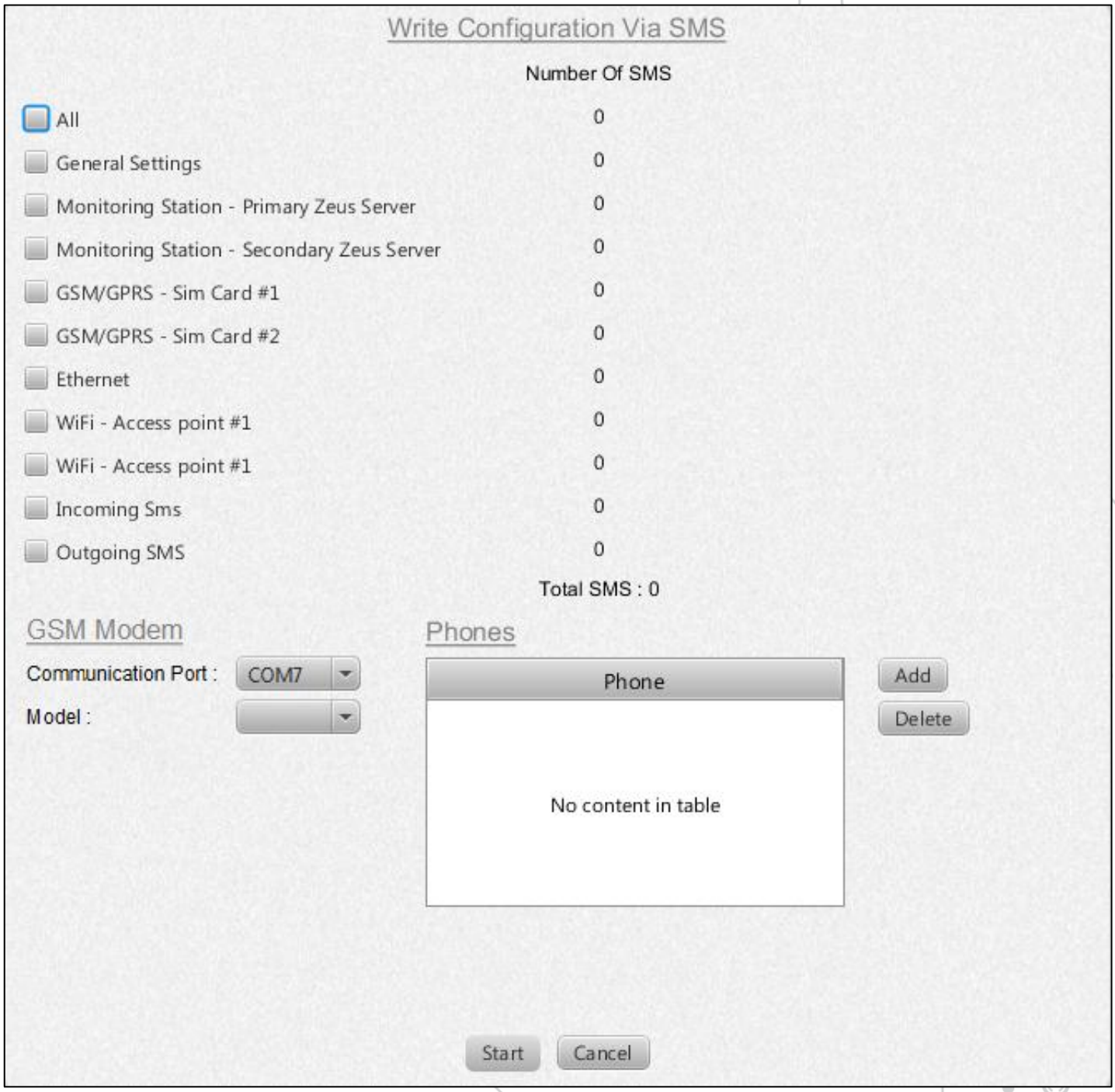
10.1. Write the Configuration Settings to Pegasus™ NX via SMS

To write the configuration settings to Pegasus™ NX via SMS

1. Open the **Pegasus™ Studio Main Screen**, and then click **Write Configuration via SMS.**

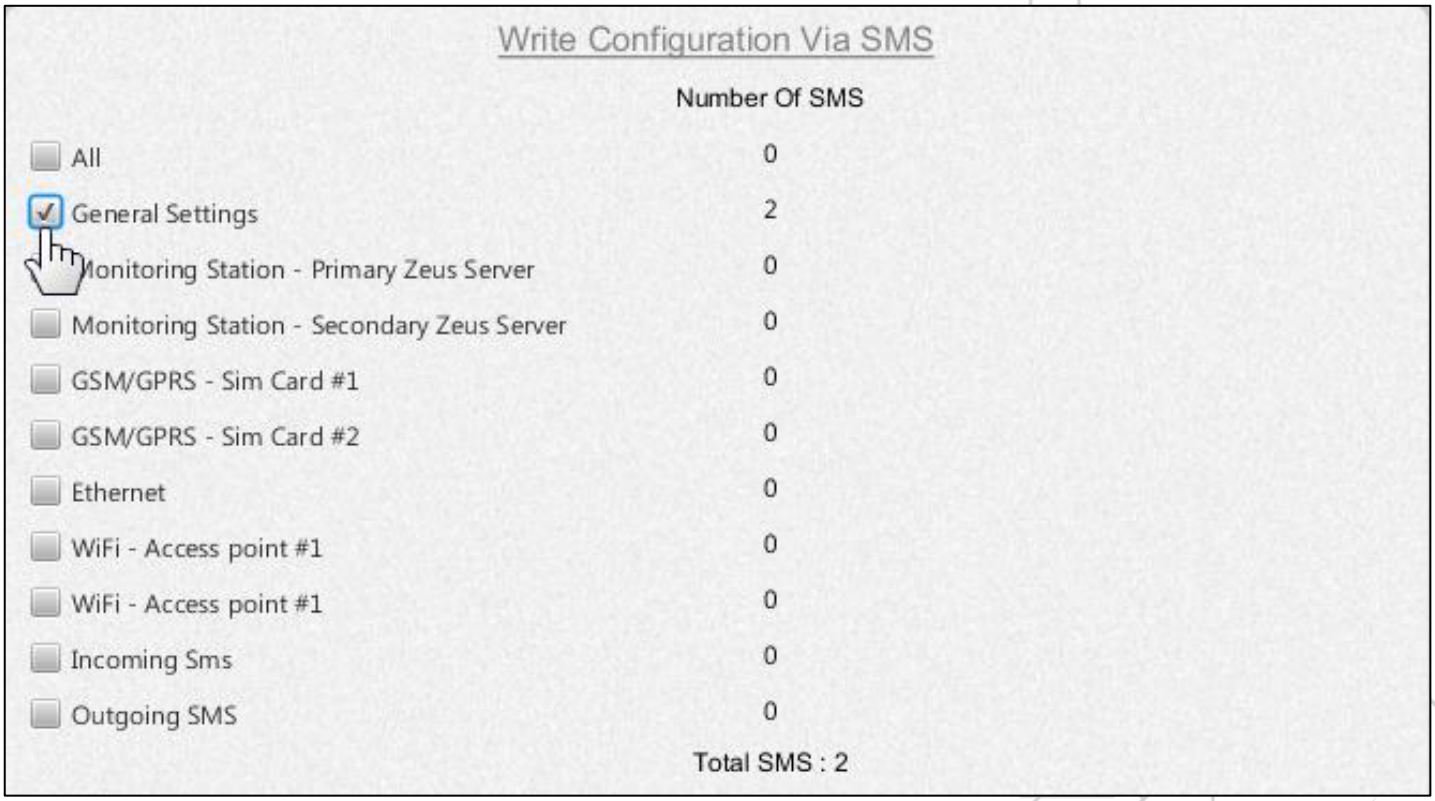


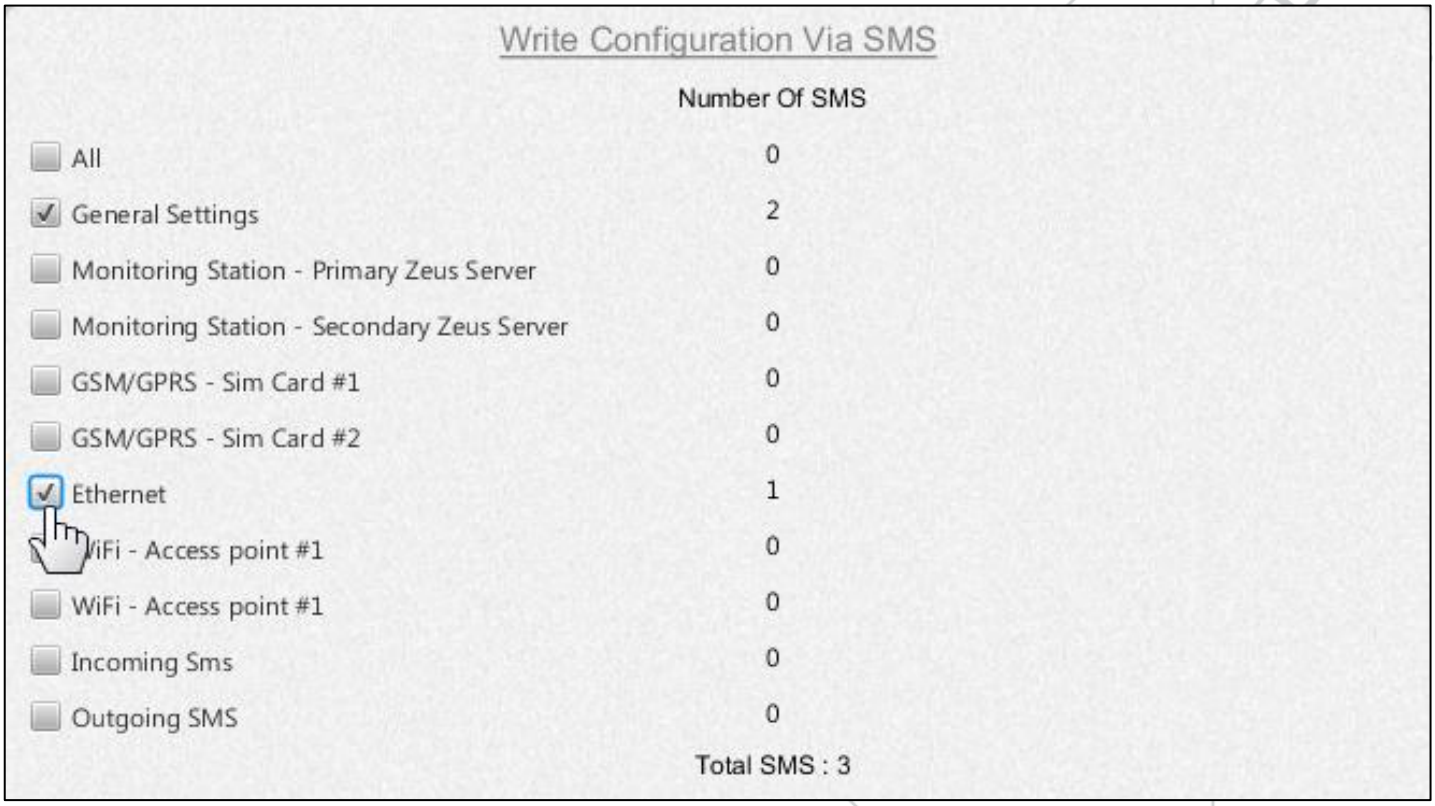
The **Write Configuration via SMS** screen is displayed.



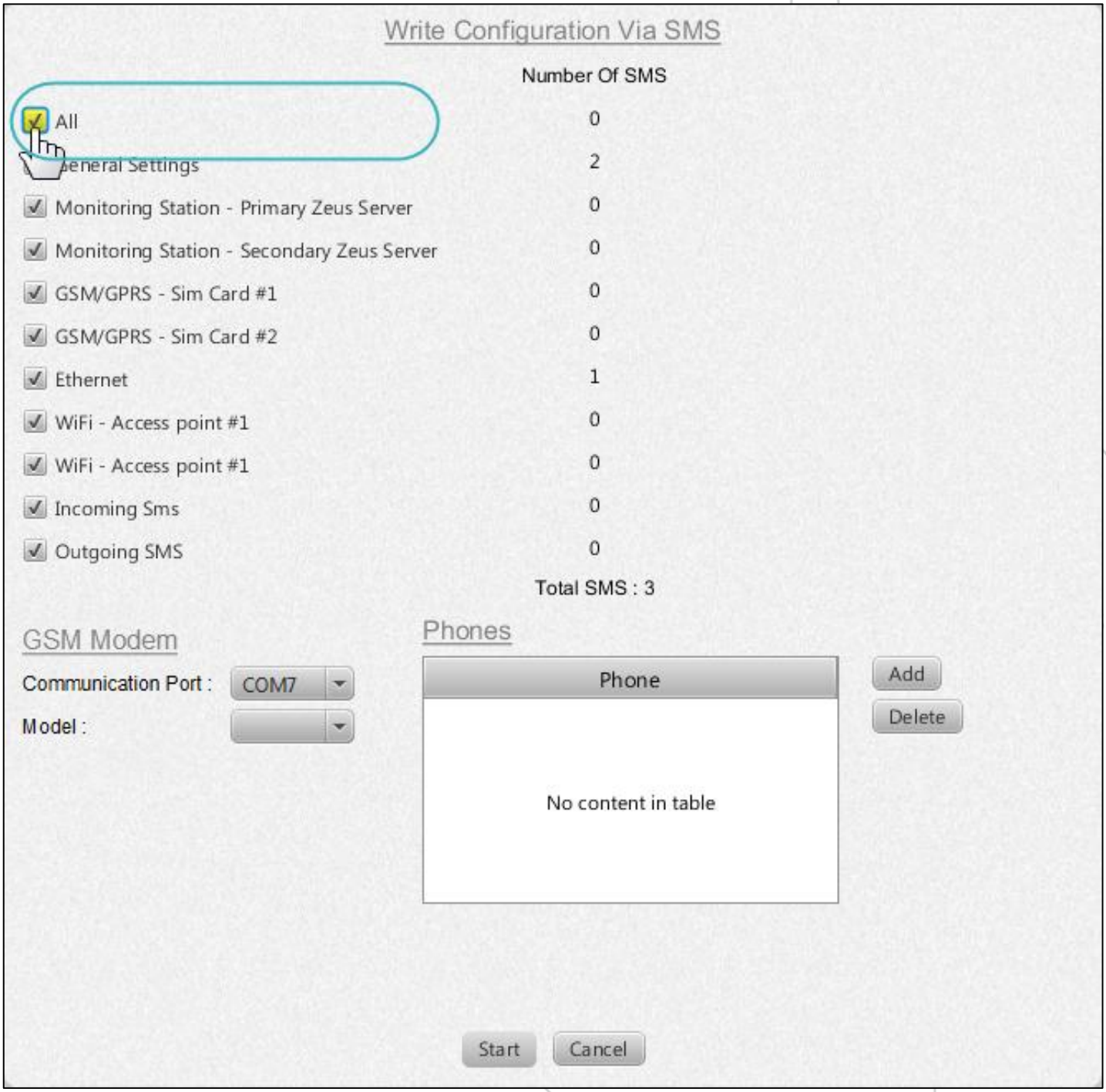
2. On the basis of your configuration settings, select the check box(es).

   Example 1: Suppose you performed Ethernet and Incoming SMS related configuration. To write the configuration settings to Pegasus™ NX via sms, in the **Write Configuartion via SMS** screen, select the **Ethernet** and **Incoming SMS** check boxes.

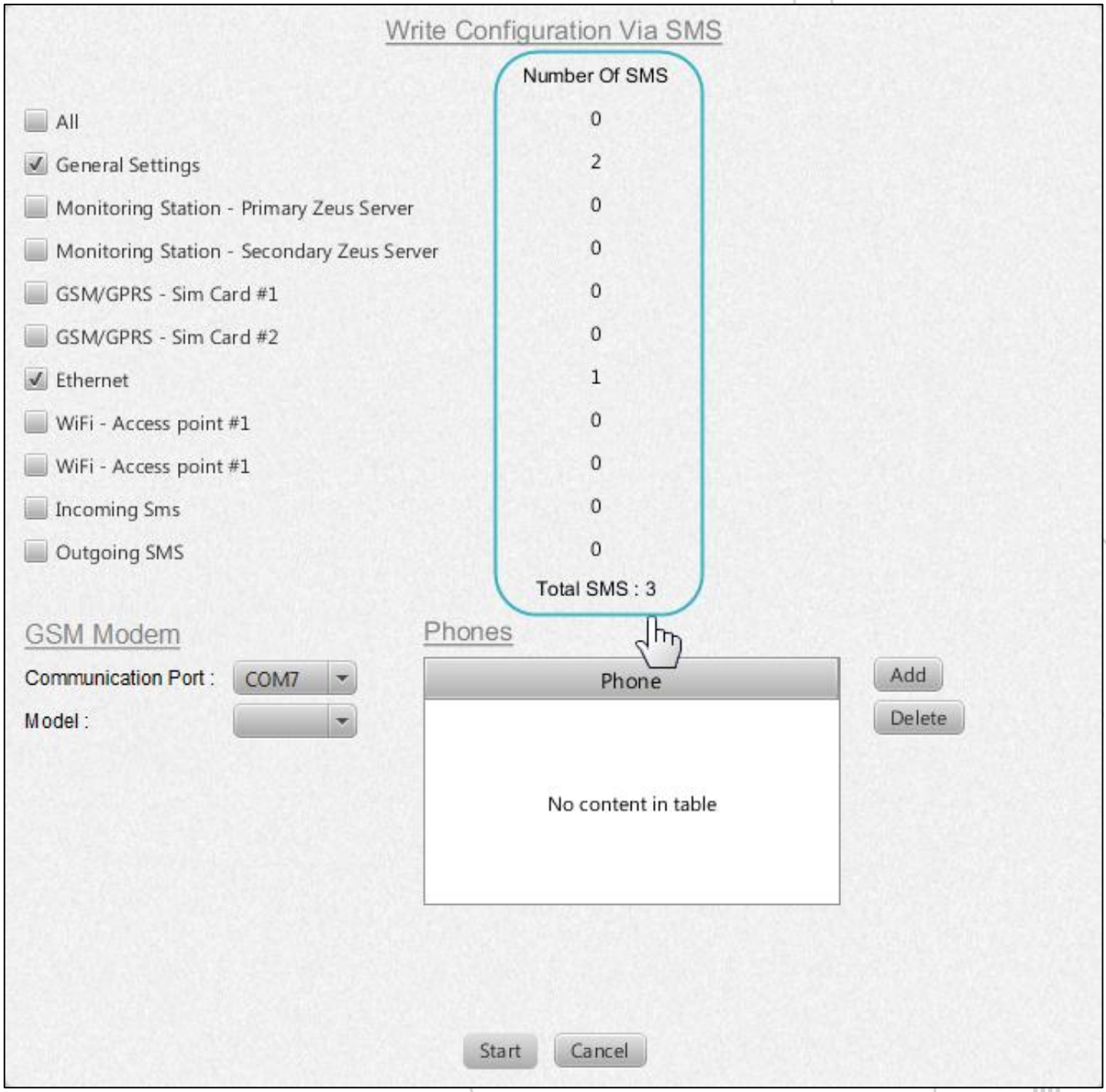

Write Configuration Via SMS
Number Of SMS
All 0
General Settings 2
Monitoring Station - Primary Zeus Server 0
Monitoring Station - Secondary Zeus Server 0
GSM/GPRS - Sim Card #1 0
GSM/GPRS - Sim Card #2 0
Ethernet 0
WiFi - Access point #1 0
WiFi - Access point #1 0
Incoming Sms 0
Outgoing SMS 0
Total SMS : 2


Write Configuration Via SMS
Number Of SMS
All 0
General Settings 2
Monitoring Station - Primary Zeus Server 0
Monitoring Station - Secondary Zeus Server 0
GSM/GPRS - Sim Card #1 0
GSM/GPRS - Sim Card #2 0
Ethernet 1
WiFi - Access point #1 0
WiFi - Access point #1 0
Incoming Sms 0
Outgoing SMS 0
Total SMS : 3

Example 2: Suppose you configured settings in all interfaces. To write the configuration settings to Pegasus™ NX via sms, in the **Write Configuartion via SMS** screen, select the **All** check box.

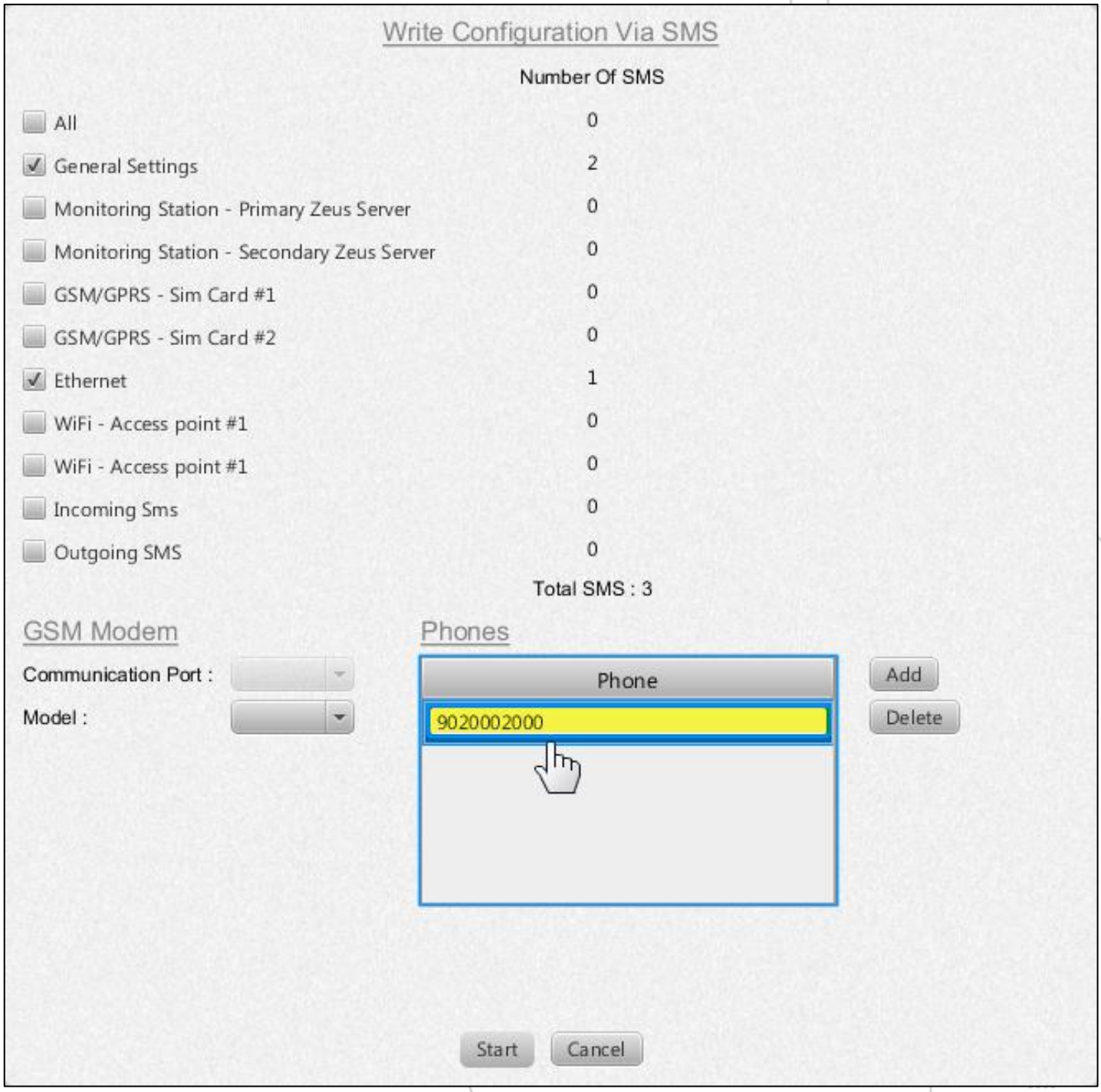


3. Under Number of SMS, the total number of SMS which are going to be sent to the device are displayed. Here the total number of SMS is 3.



4. To add the Phone number(s) of the device(s) which are going to receive the configuration settings via SMS, click the **Add** button.

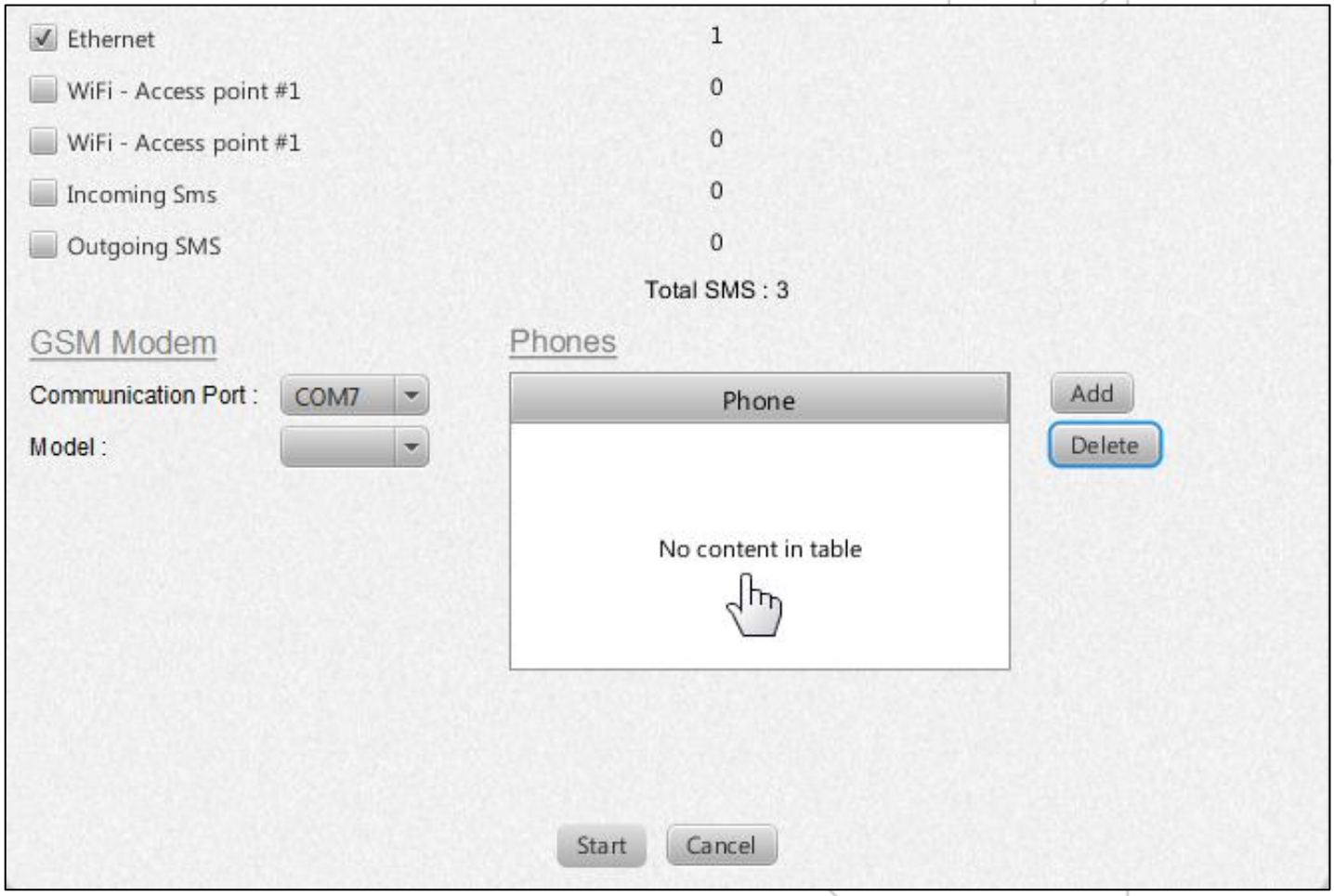
   In the **Phone** text box, type-in the first phone number of the device.



Likewise, you can configure more phone numbers.

5. To delete a phone number, select the phone number, and then click the **Delete** button.

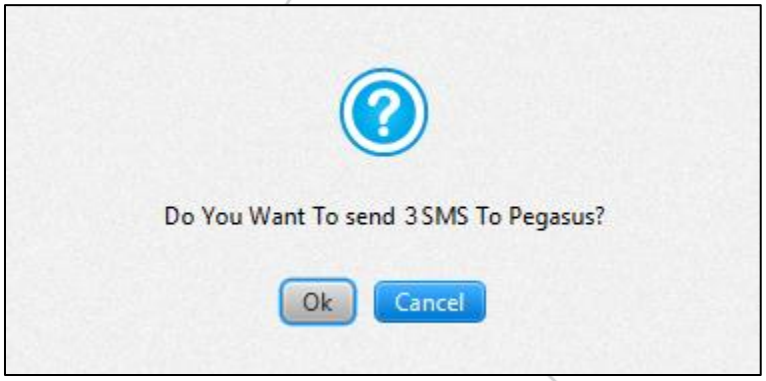
The selected phone number is deleted.



6. In the **Communication Port** drop-down box, select the port to which the gsm modem is connected.

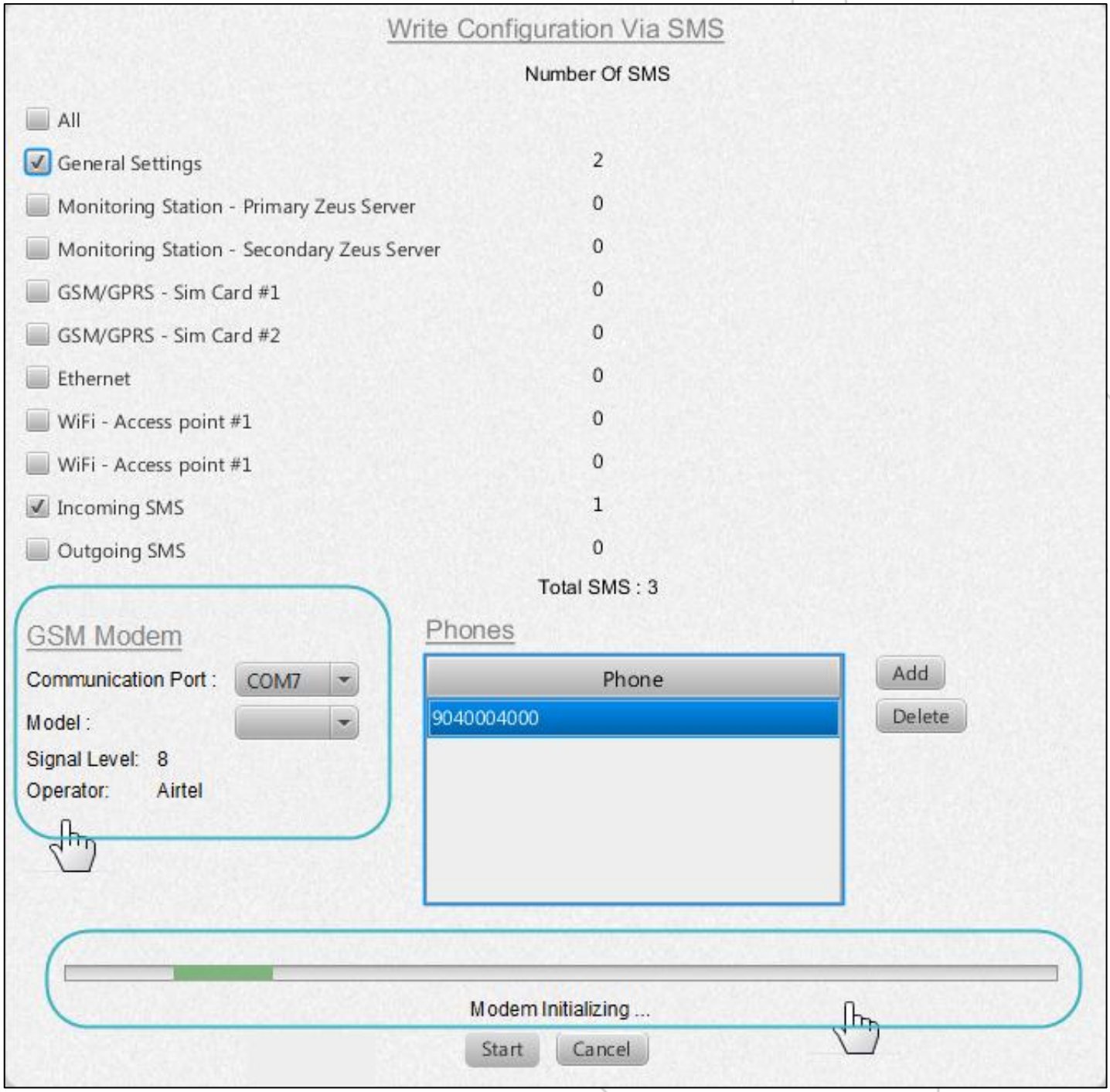
7. Click the **Start** button.

   A message box is displayed saying. “Do You Want to Send 3 SMS to Pegasus?

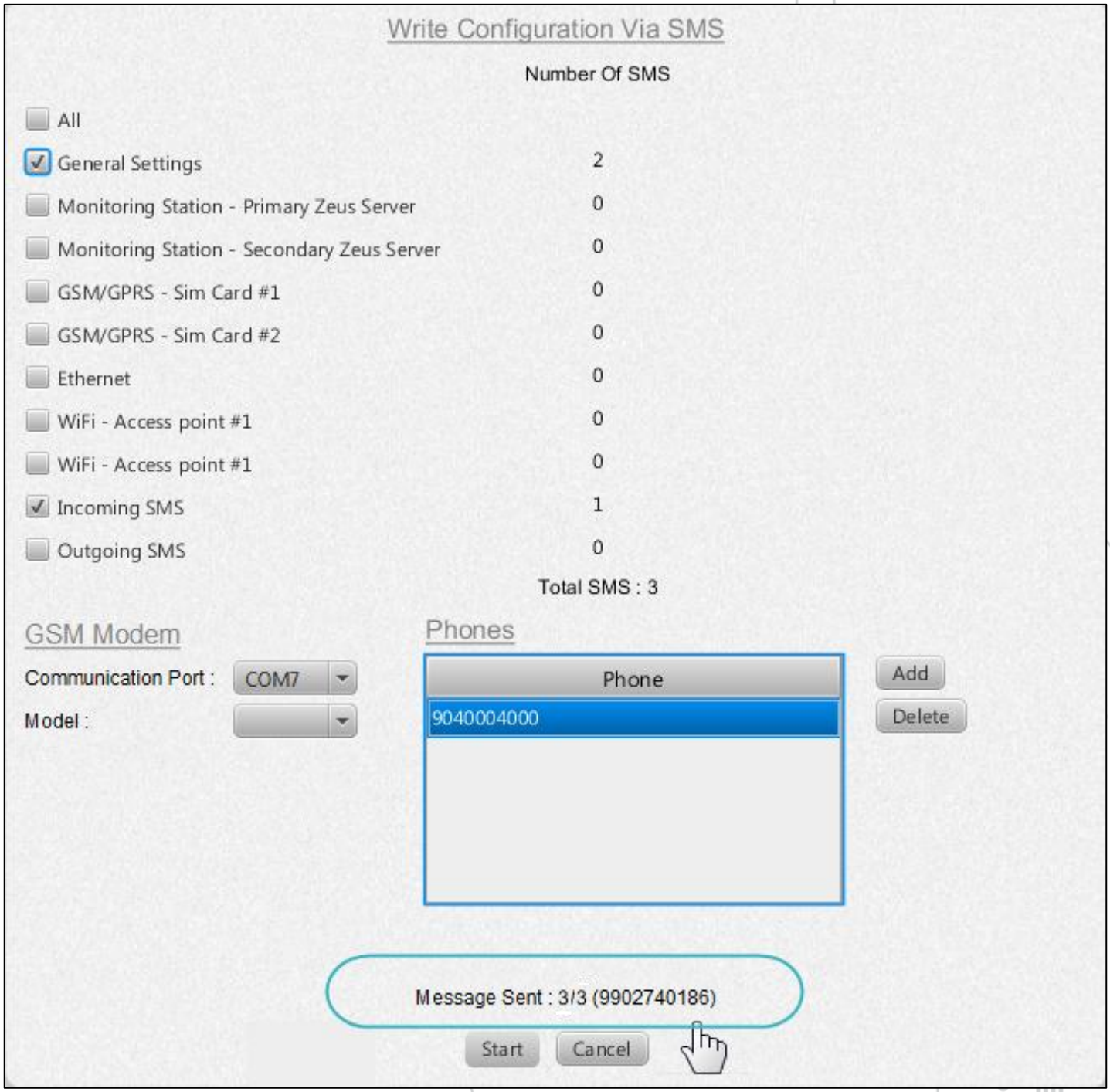


8. Click the **OK** button.

The modem initializing and configuration writing progress is displayed via the progress bar. Under GSM Modem, gsm signal level and operator details are displayed.



After successful writing of the configuration settings to the device via sms, a confirmation message is displayed saying, “Message Sent: 3/3 (9902740186).


Write Configuration Via SMS
Number Of SMS
All
General Settings 2
Monitoring Station - Primary Zeus Server 0
Monitoring Station - Secondary Zeus Server 0
GSM/GPRS - Sim Card #1 0
GSM/GPRS - Sim Card #2 0
Ethernet 0
WiFi - Access point #1 0
WiFi - Access point #1 0
Incoming SMS 1
Outgoing SMS 0
Total SMS : 3
GSM Modem
Communication Port : COM7
Model :
Phones
Phone
9040004000
Add
Delete
Message Sent : 3/3 (9902740186)
Start
Cancel

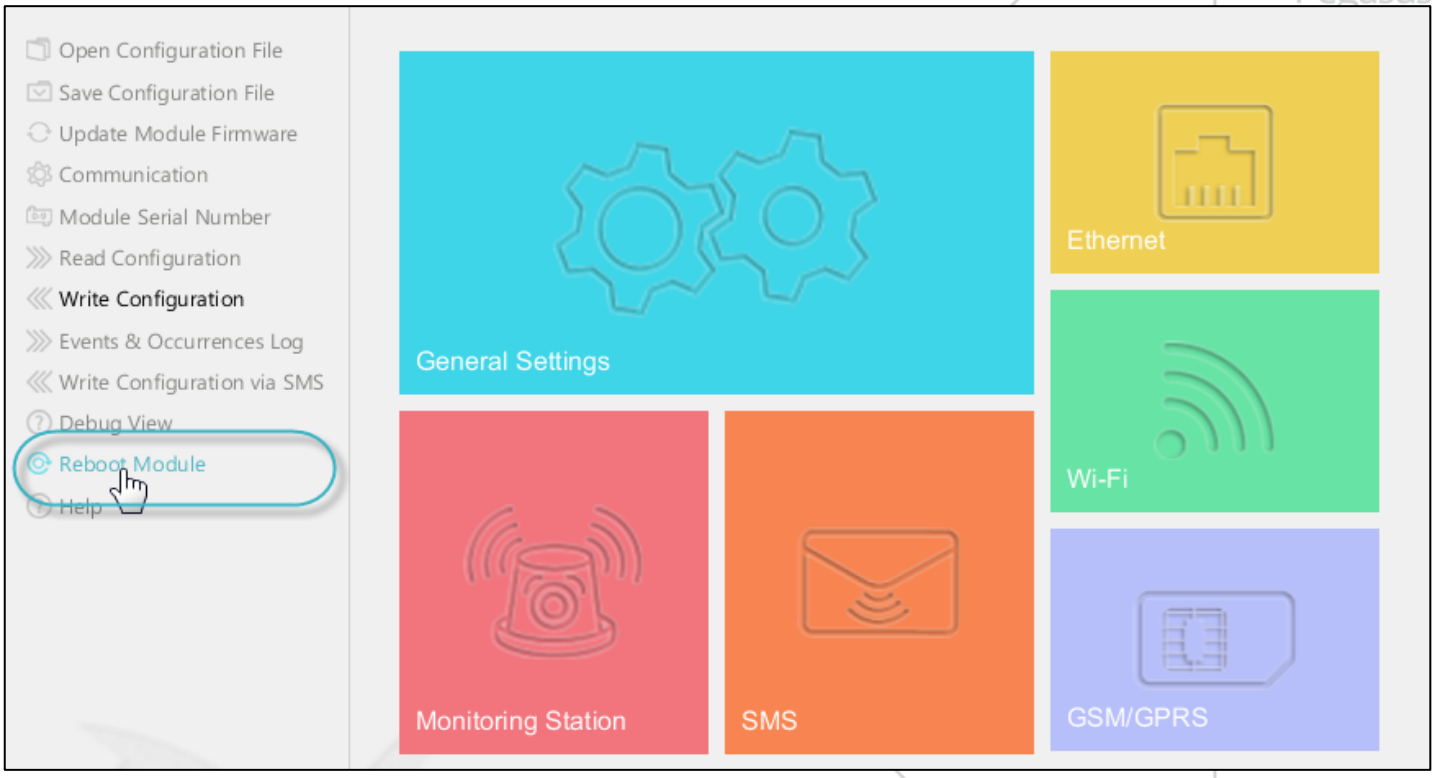
11 Reboot Module

Once the configuration is written to your Pegasus™ Module, it is stored in its flash memory. Module reboot is required to make the configuration settings functional.

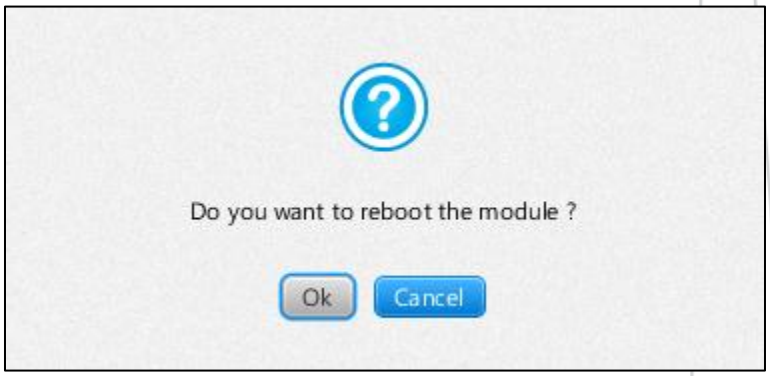
11.1. Reboot Your Pegasus™ Module

To reboot your Pegasus™ module

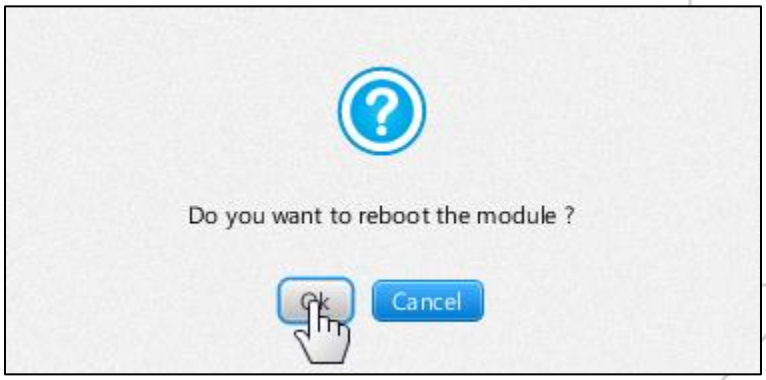
1. Open the **Pegasus™ Studio Main Screen,** and then click **Reboot Module**.



A message box saying, “Do you want to reboot the module?” is displayed.



2. Click the **OK** button.



Your configuration is now applied and functional.

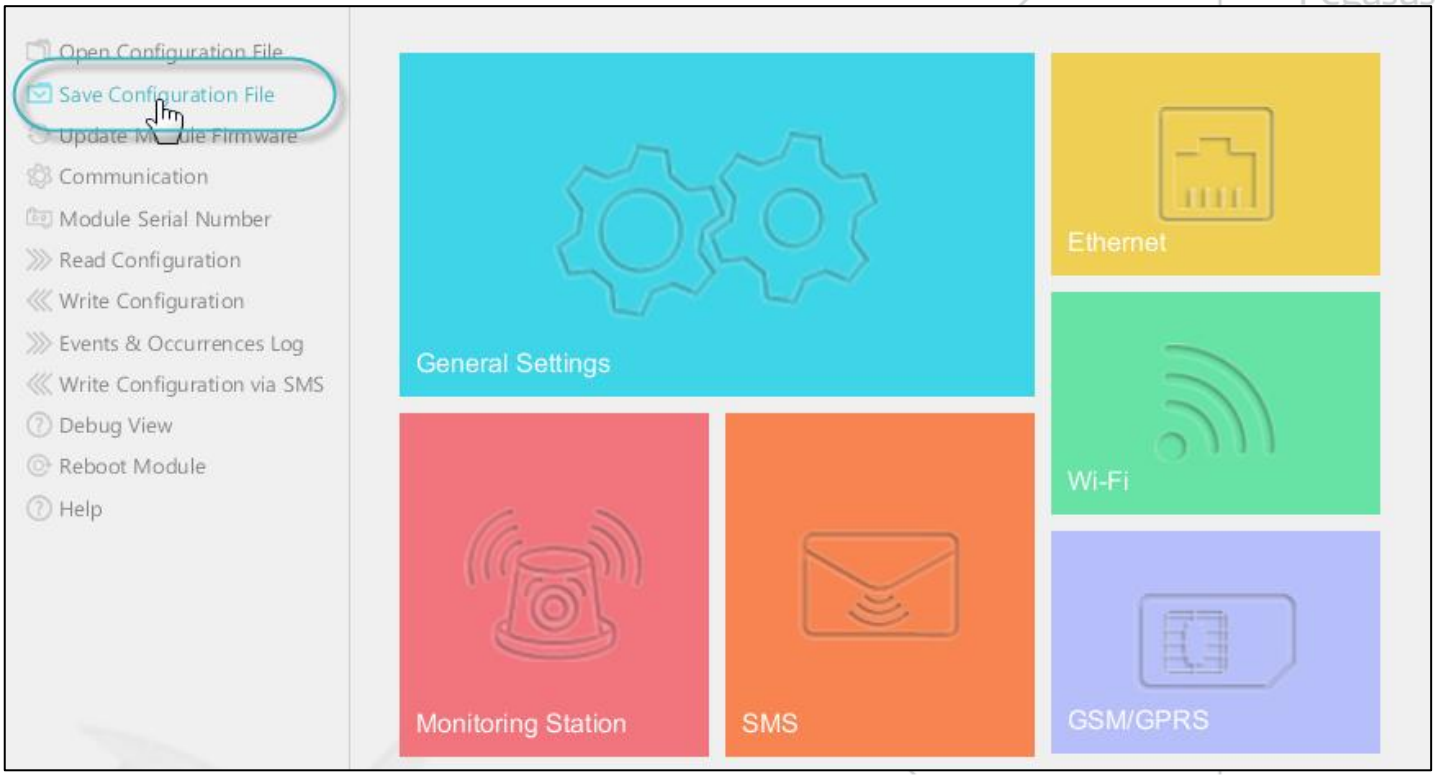
12 Save Configuration File

The **Save Configuration File** feature allows you to save the configuration file with Config file(*.bin) as the file type in your hard disk drive.

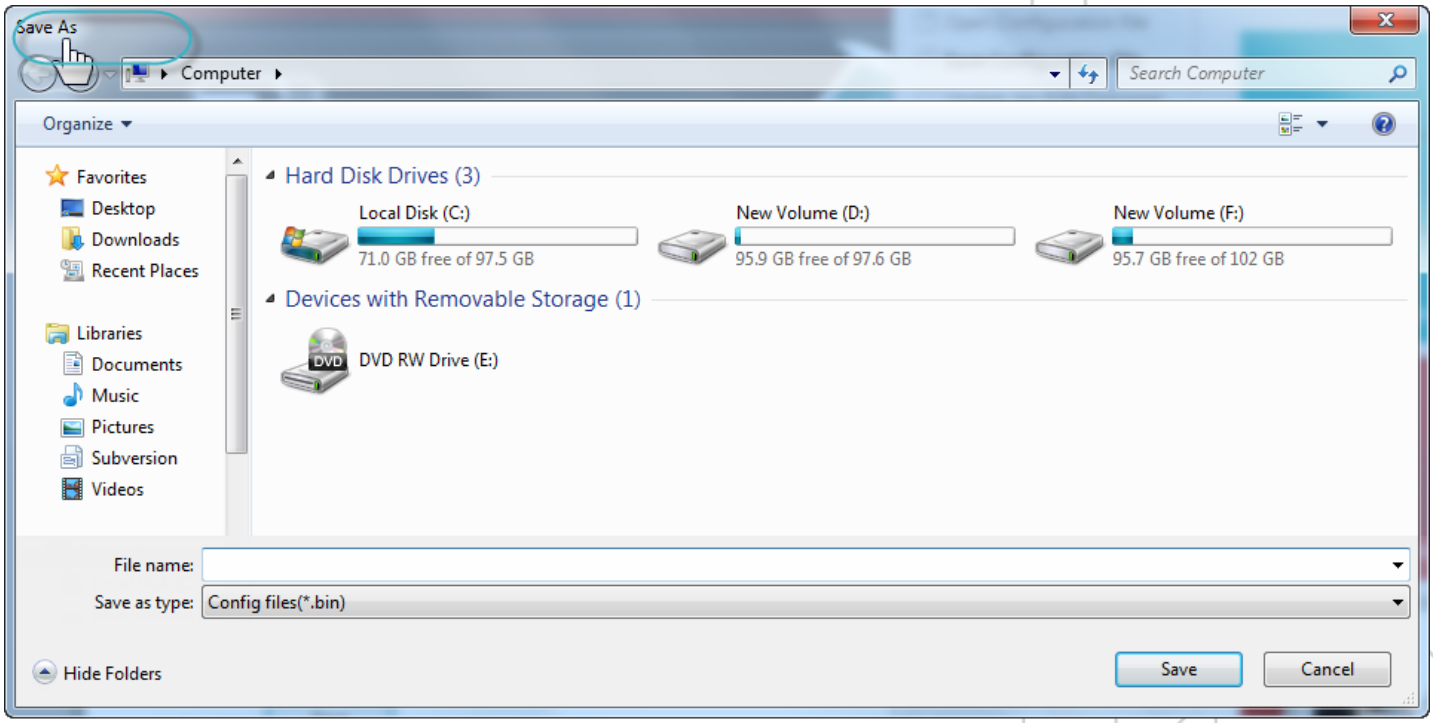
12.1. Save the Pegasus™ Studio Configuration File

To save the Pegasus™ Studio configuration

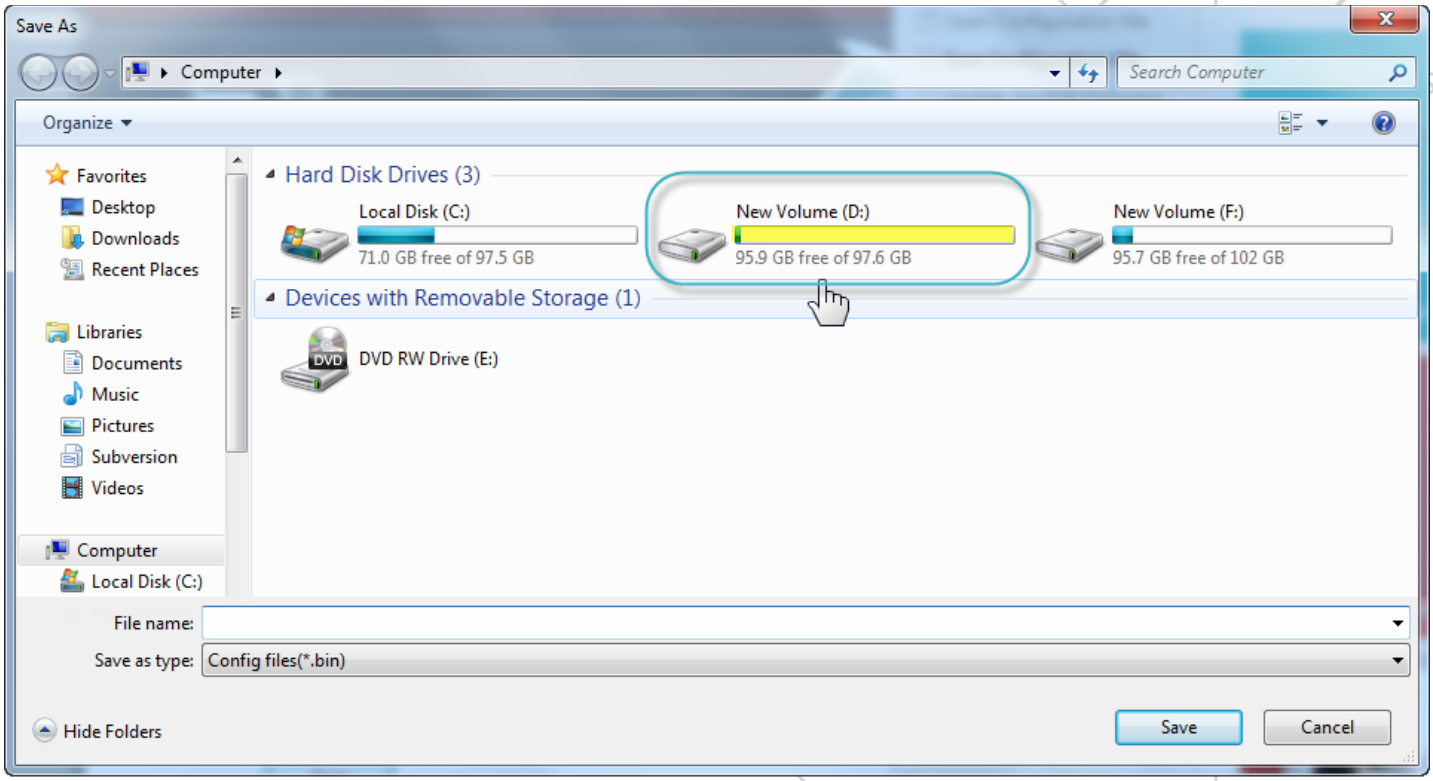
1. Open the **Pegasus™ Studio Main Screen,** and then click **Save Configuration File**.



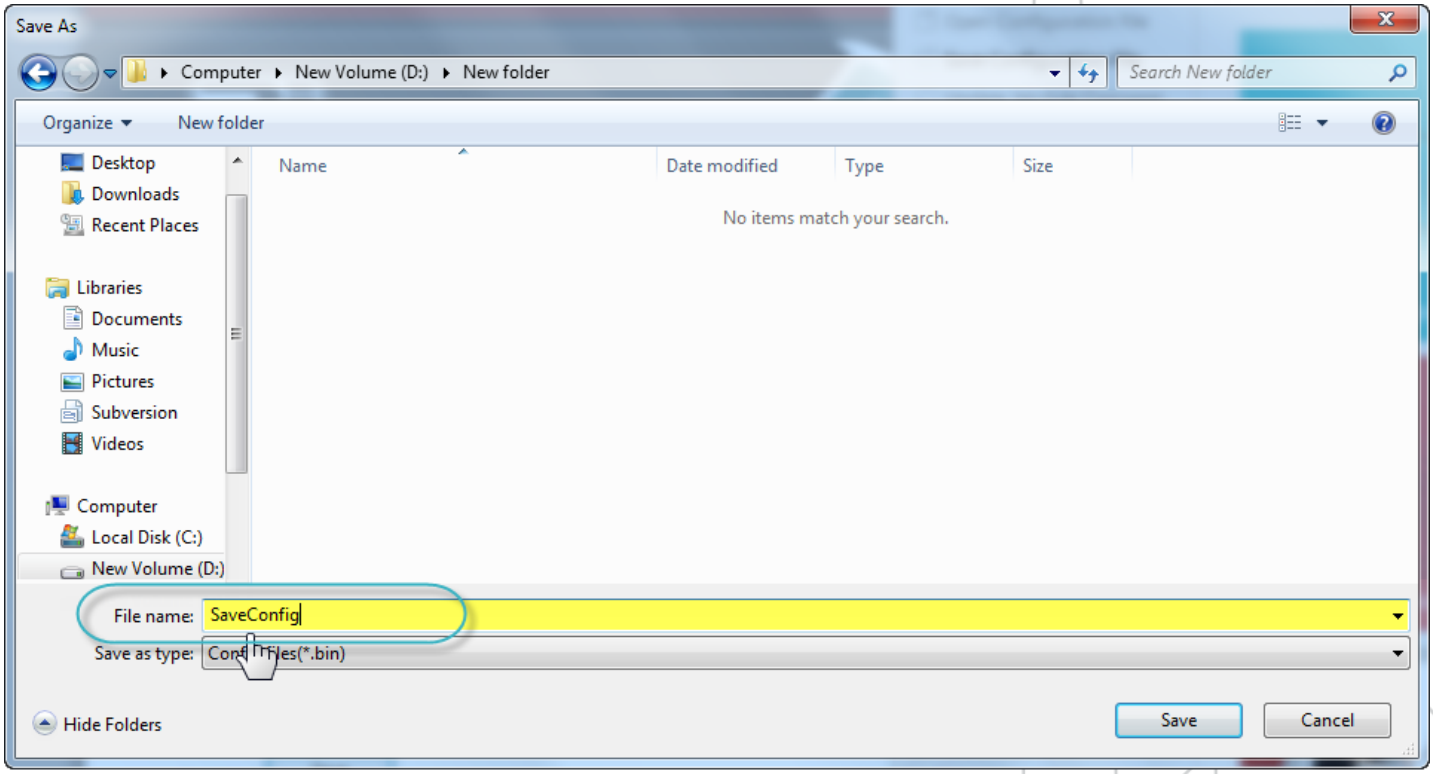
The **Save As** dialog box is displayed as shown below.



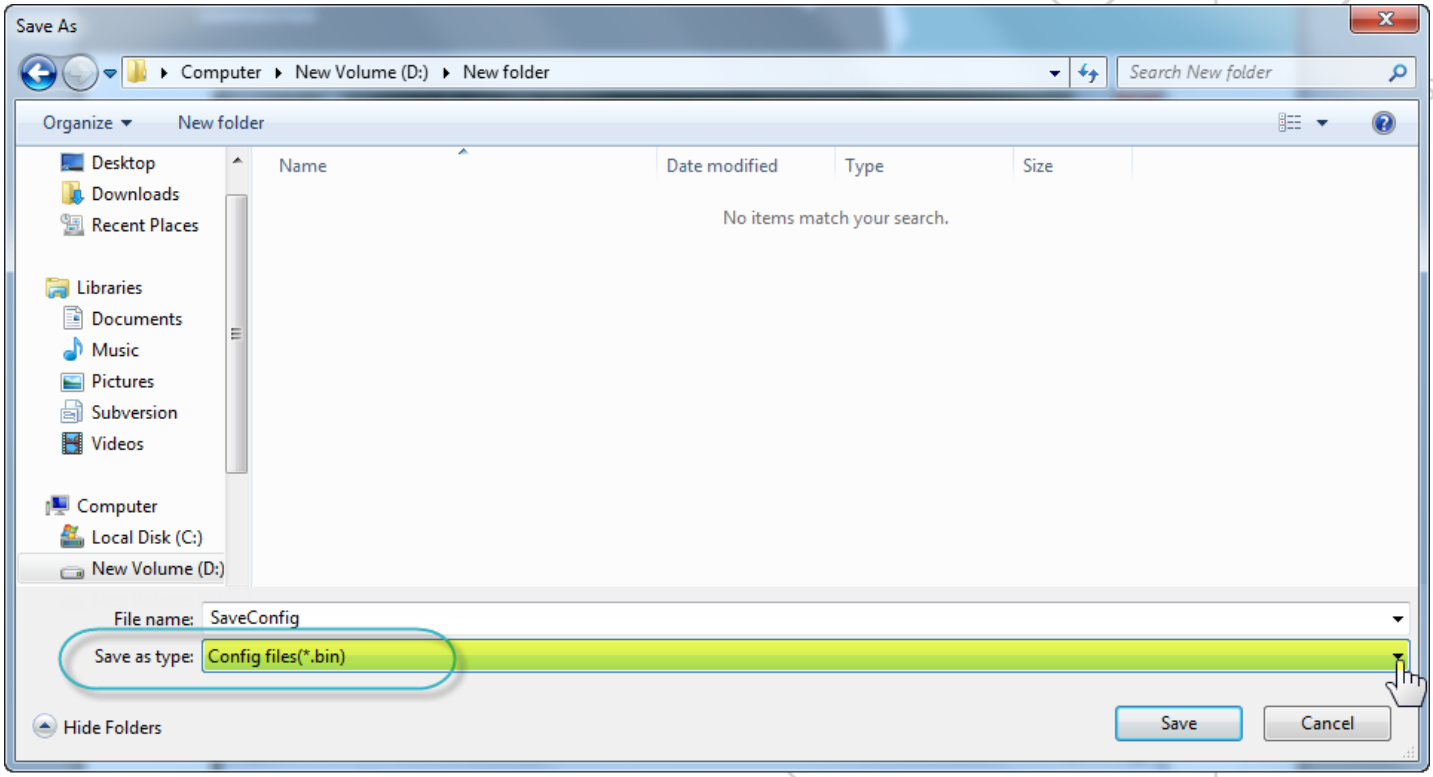
2. Select the location in your computer hard drive (C:), (D:), (F:), etc where you want to save the configuration file.

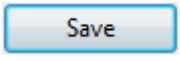


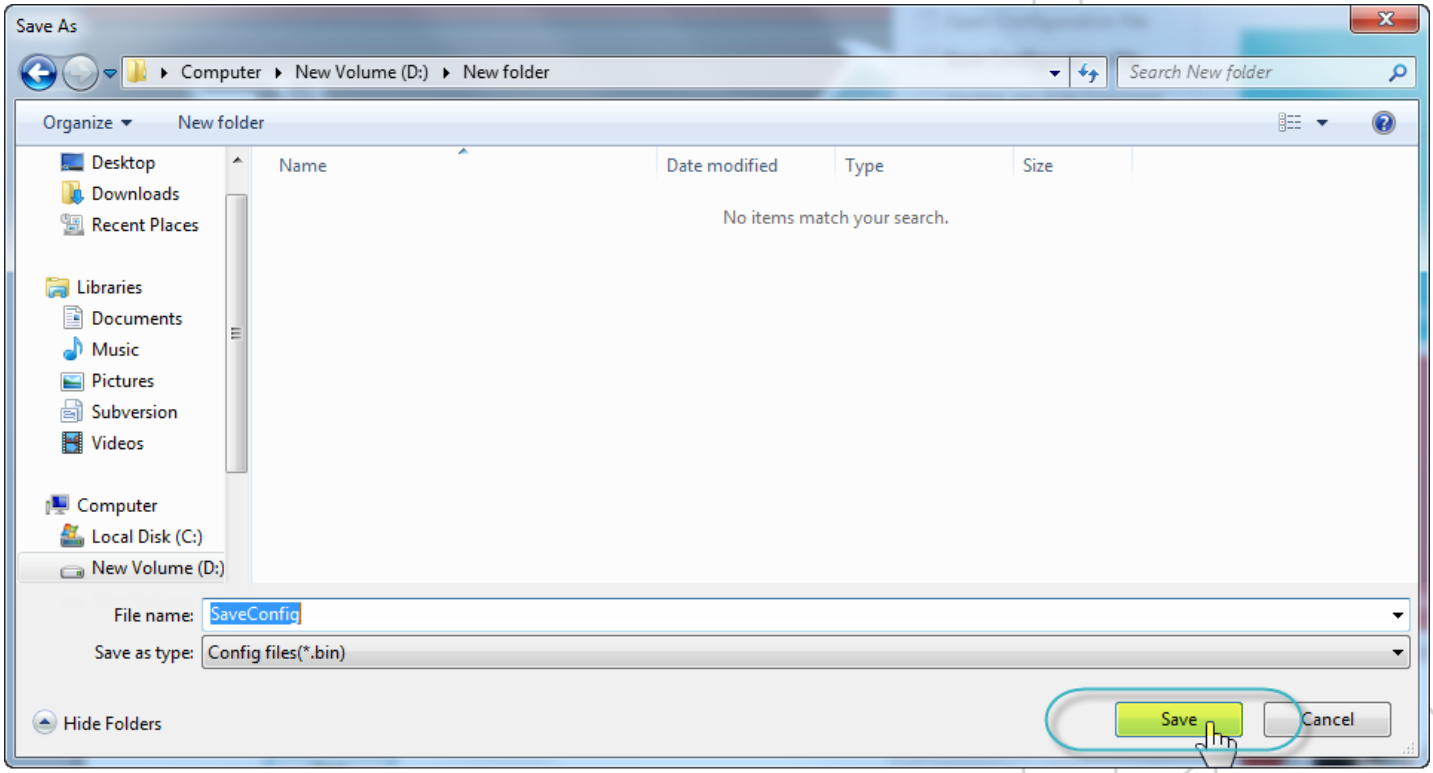
3. In the **File name** box, type the name of the configuration file**.**



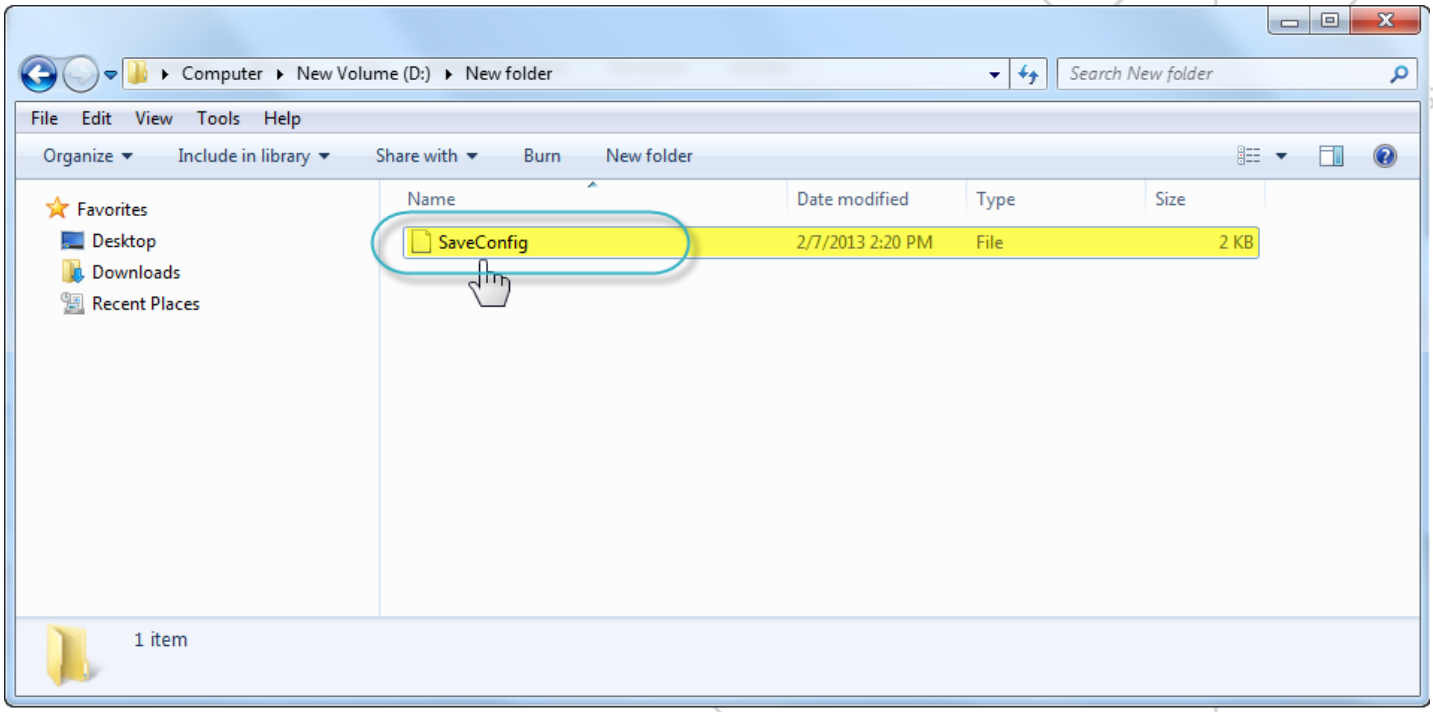
4. In the **Save as type** box, select **Config file(*.bin)** as the file type.



5. Click the **Save**  button.



Your current configuration is saved successfully.



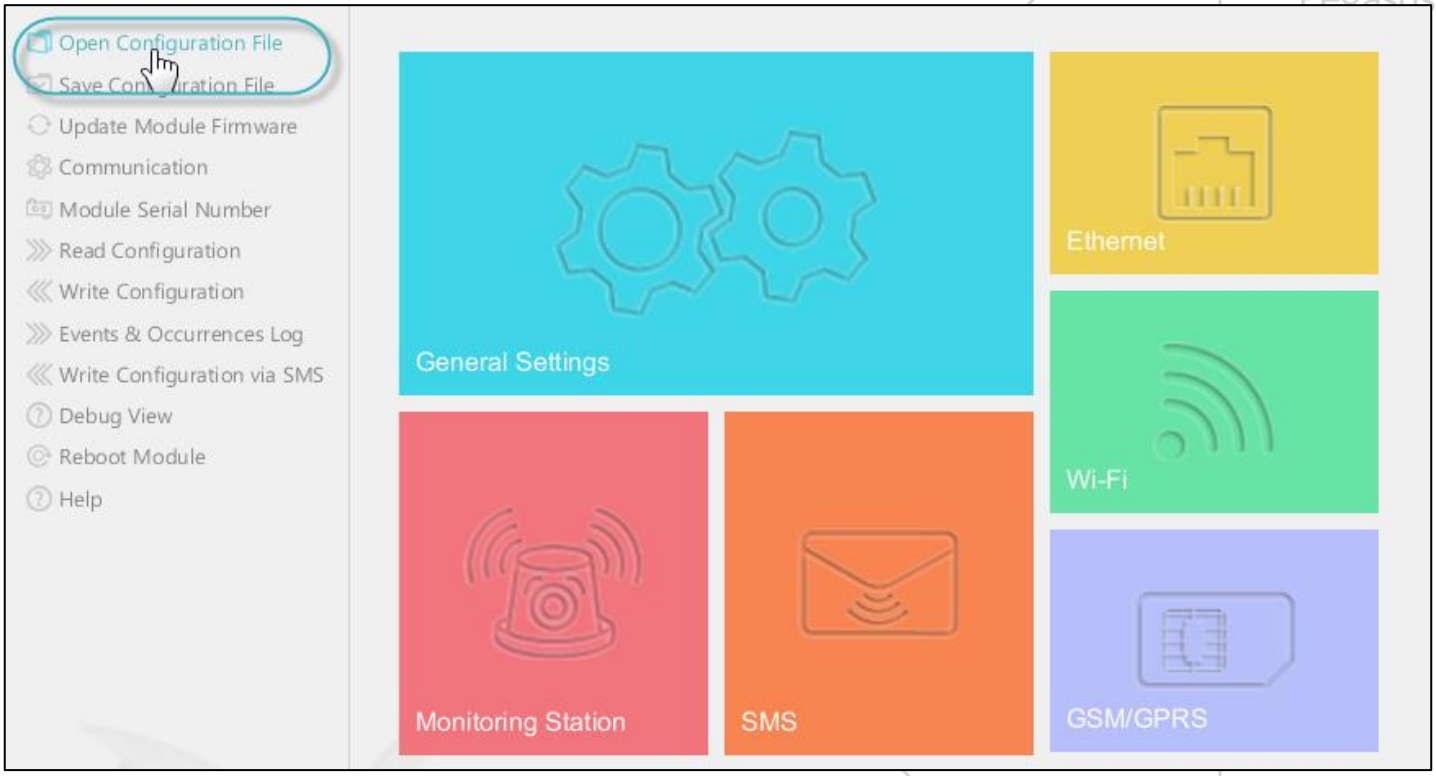
13 Open Configuration File

The **Open Configuration File** feature allows you to open a previously saved configuration file with **Config file(*.bin)** extension from hard drive.

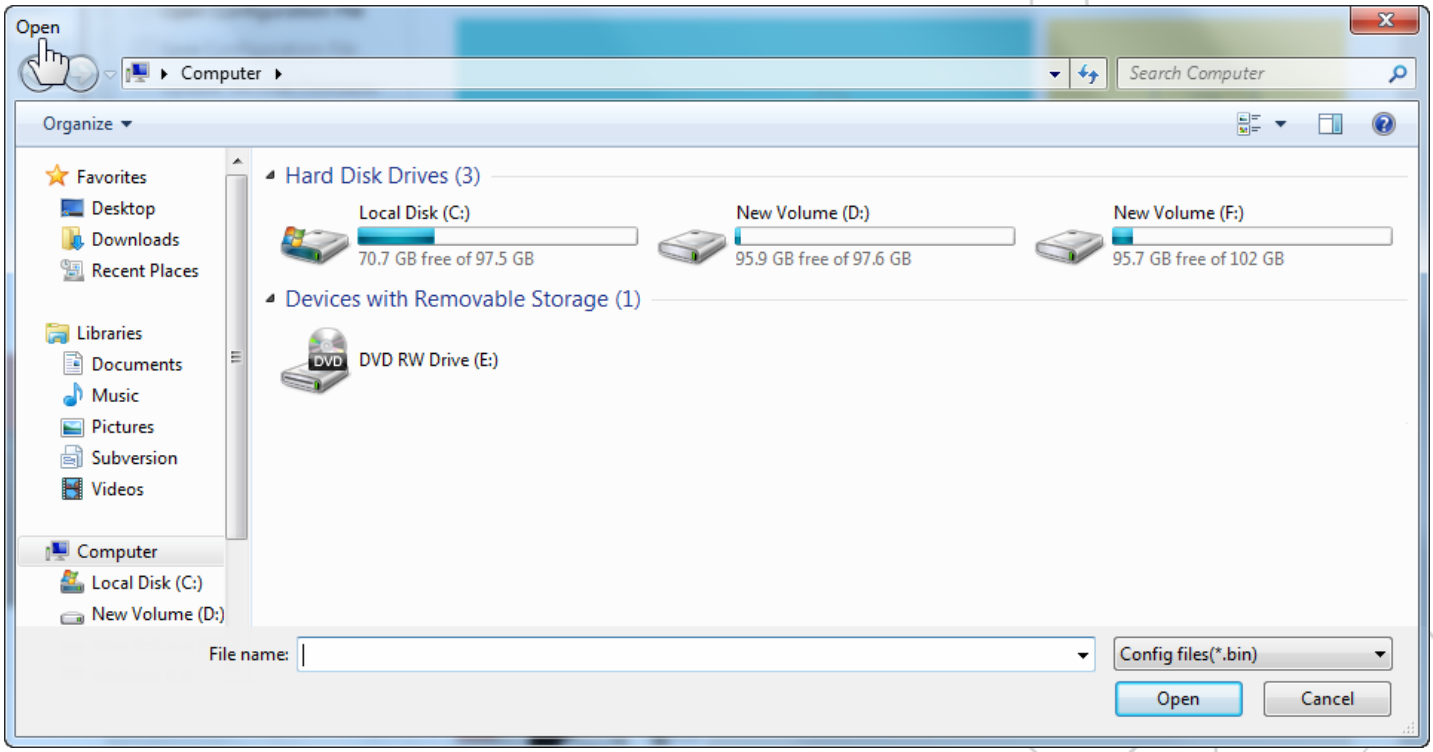
13.1. Open a Previously Saved Configuration File

To open a previously saved configuration file

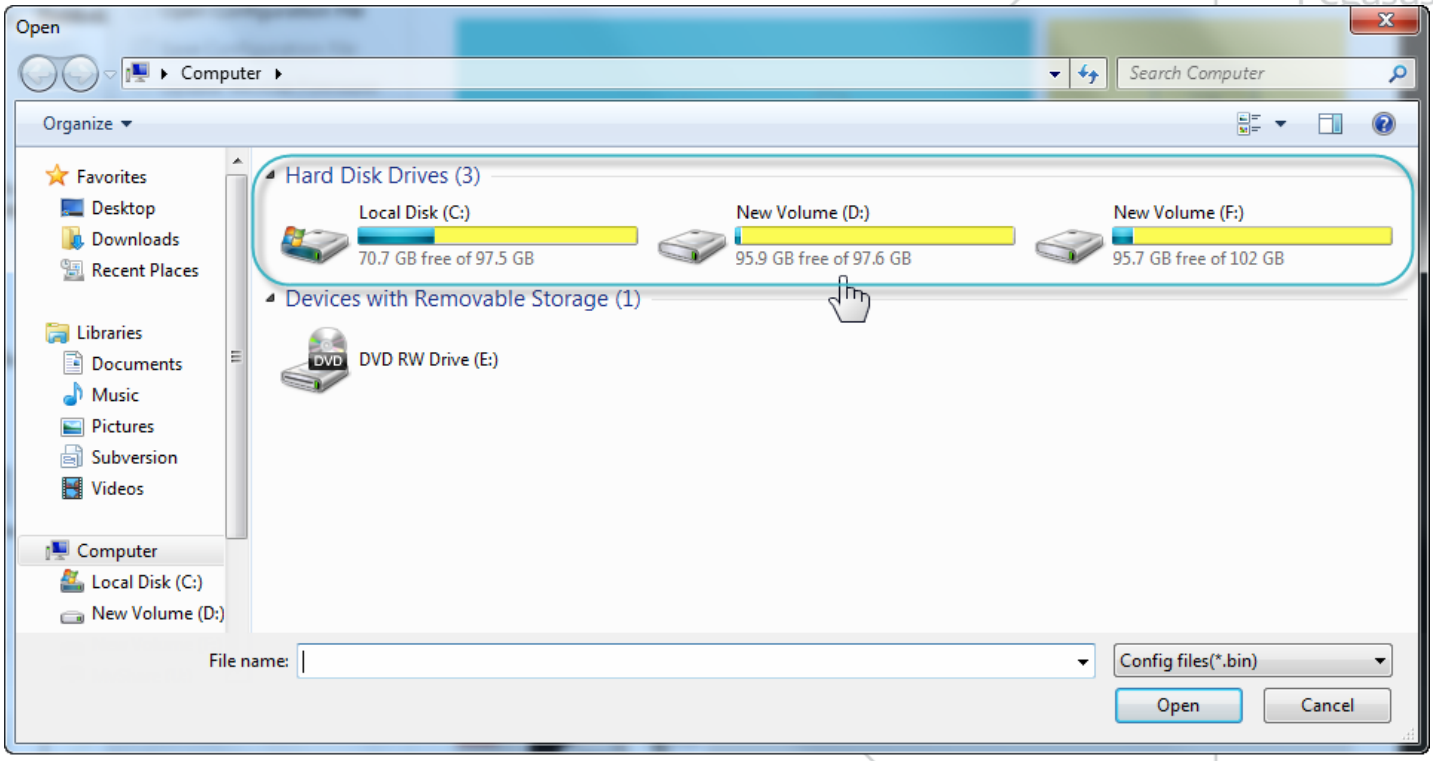
1. Open the **Pegasus™ Studio Main Screen,** and then click **Open Configuration File**.



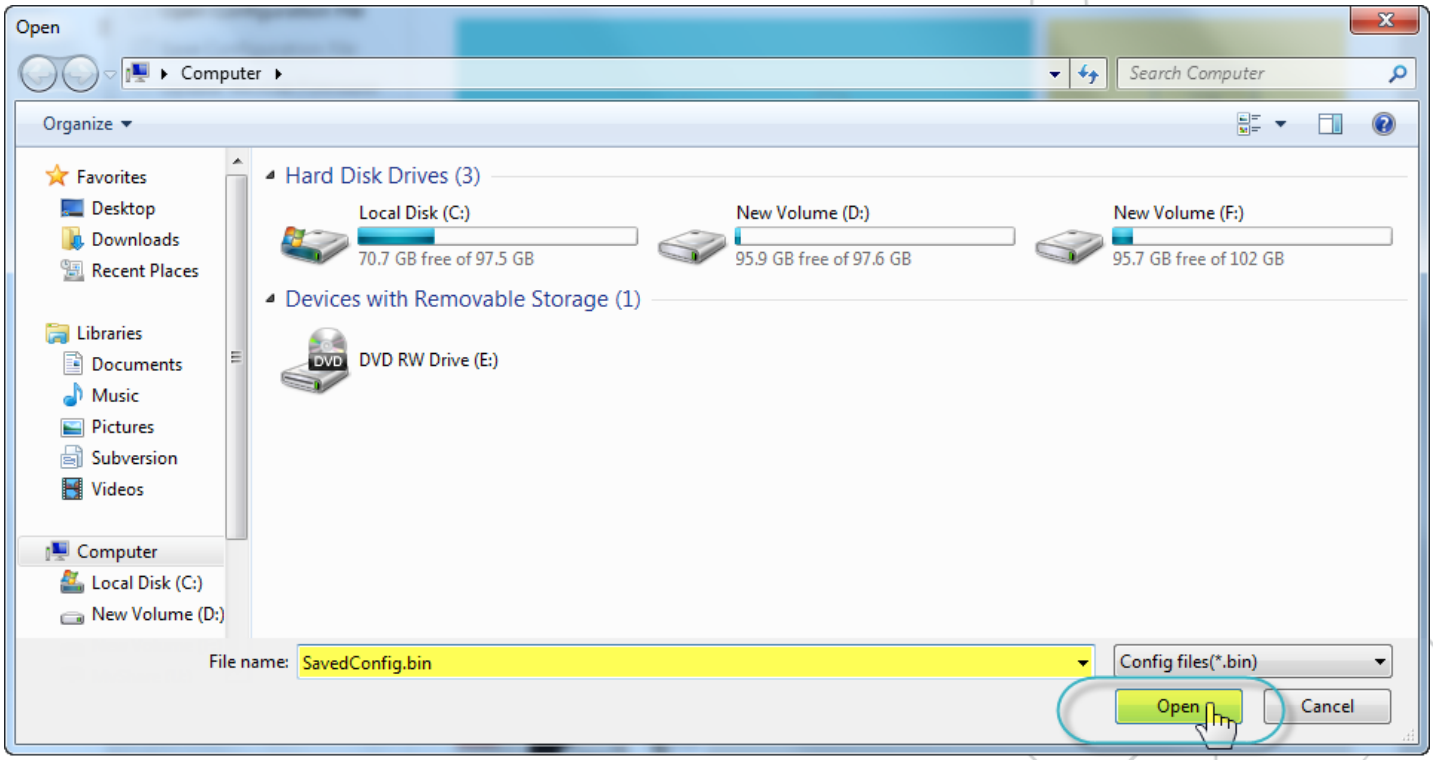
The **Open** dialog box is displayed.



2. Browse the Configuration File (with *.bin extension) in your computer hard disk drives: (C:), (D:), (F:), etc. where you saved it previously.



3. Select the configuration file, and then click the **Open** button.



The selected configuration is loaded into Pegasus™ Studio.

Note:

Reboot module after opening a previously saved configuration to your Pegasus™ Module, refer the **Reboot Module** chapter.

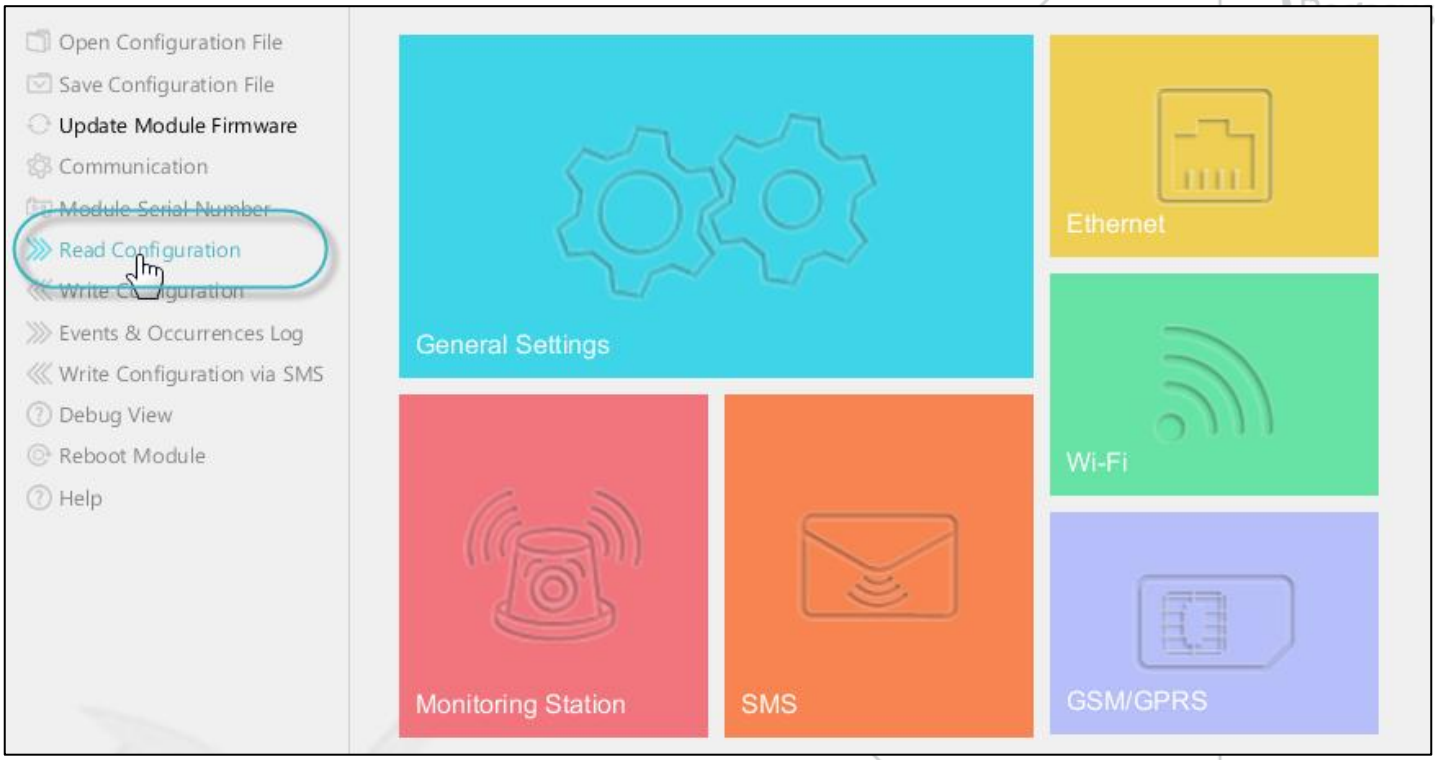
14 Read Configuration

The **Read Configuration** feature allows you to read the current configuration settings and save it to file for future use.

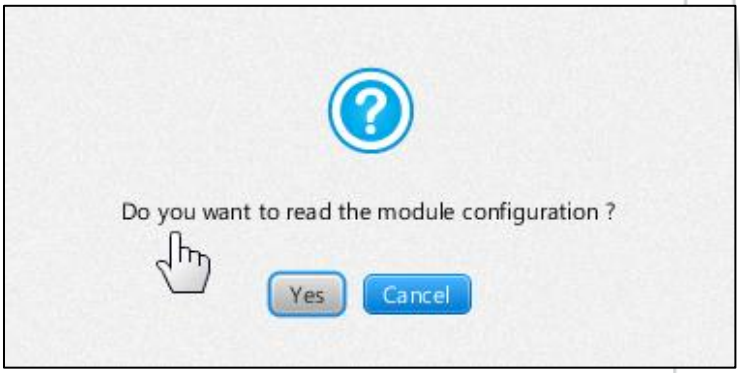
14.1. Save the Current Configuration Settings to File

To save the current configuration settings to file

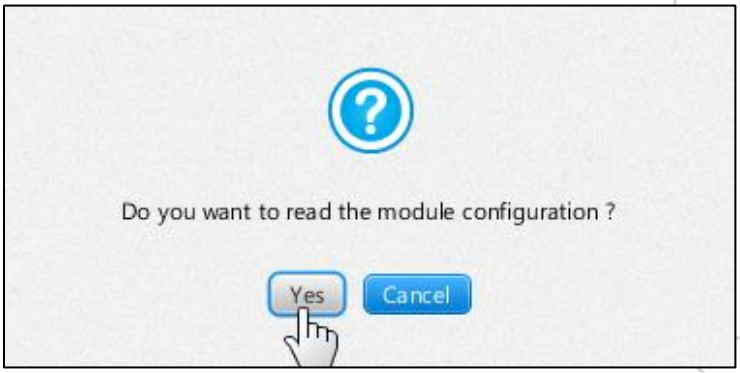
1. Open **Pegasus™ Studio,** and then click **Read Configuration.**



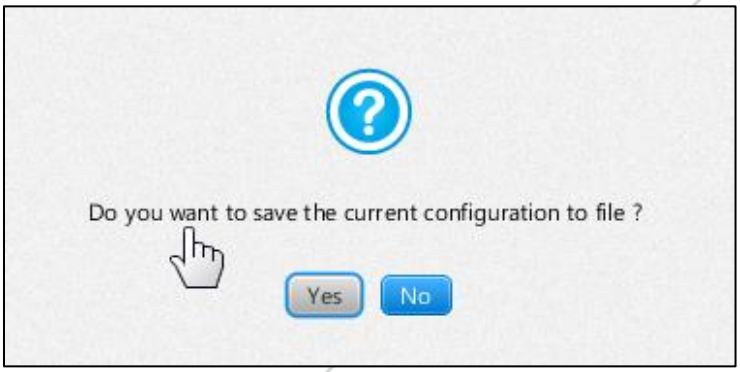
A message box saying, “Do you want to read the module configuration?” is displayed.



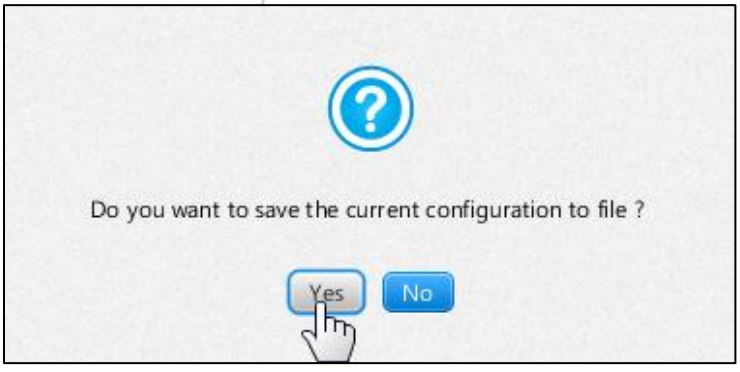
2. To proceed, click the **Yes** button.



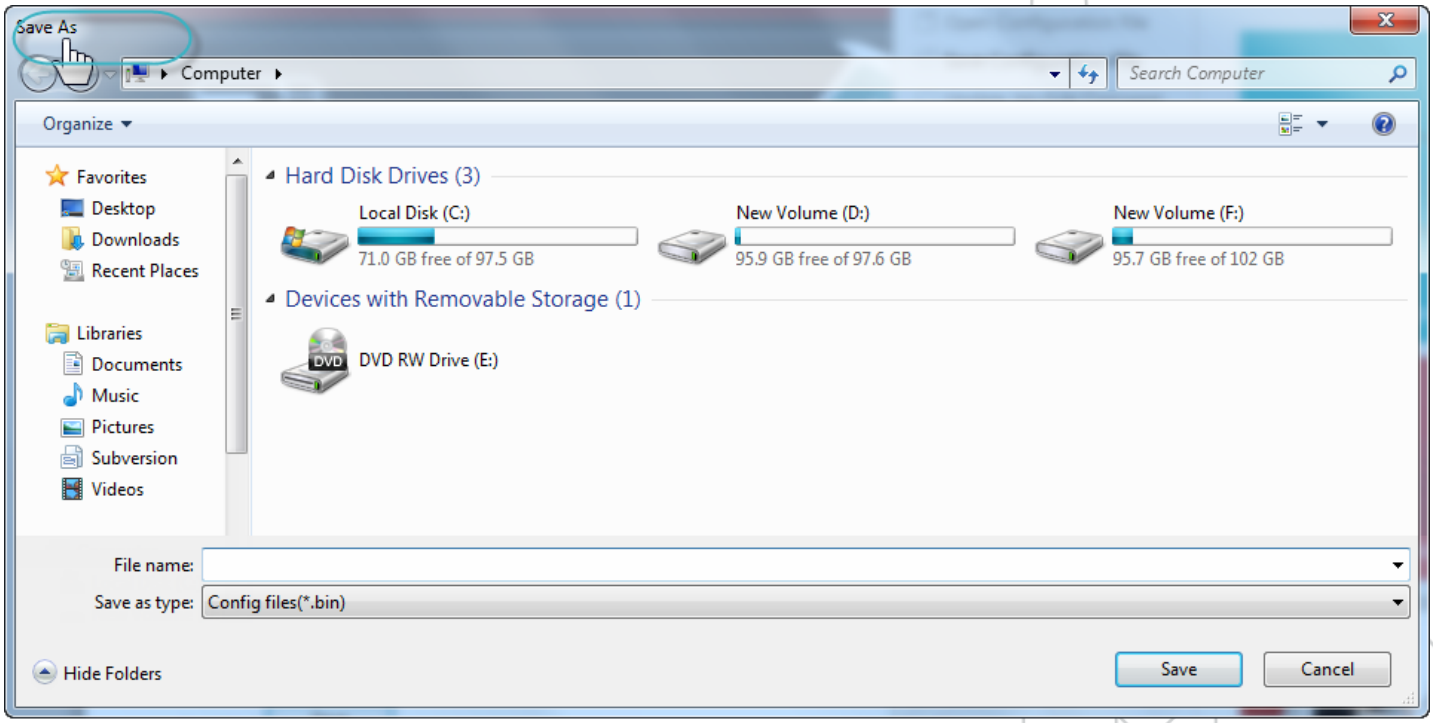
A message box is displayed saying, “Do you want to save the current configuration to file?”



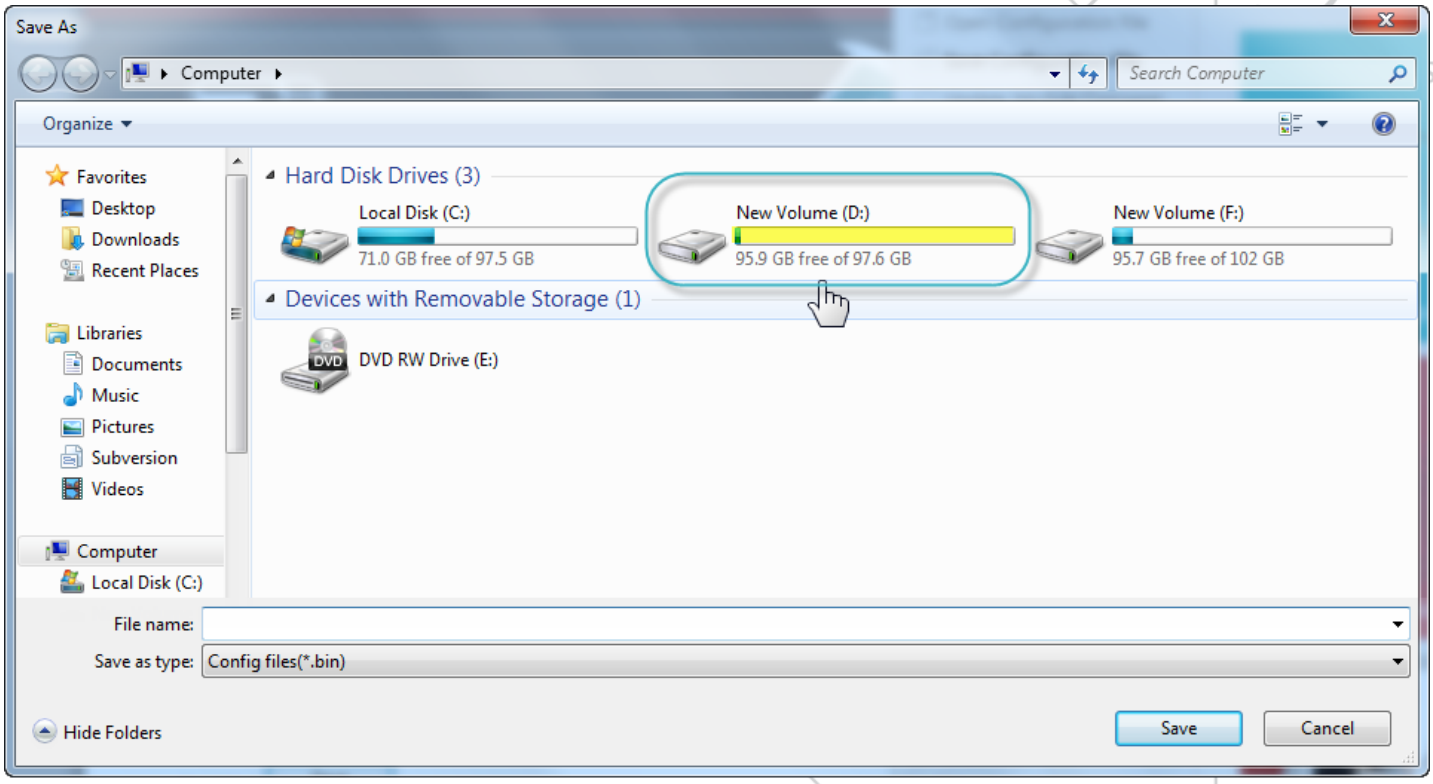
3. To proceed, click the **Yes** button.



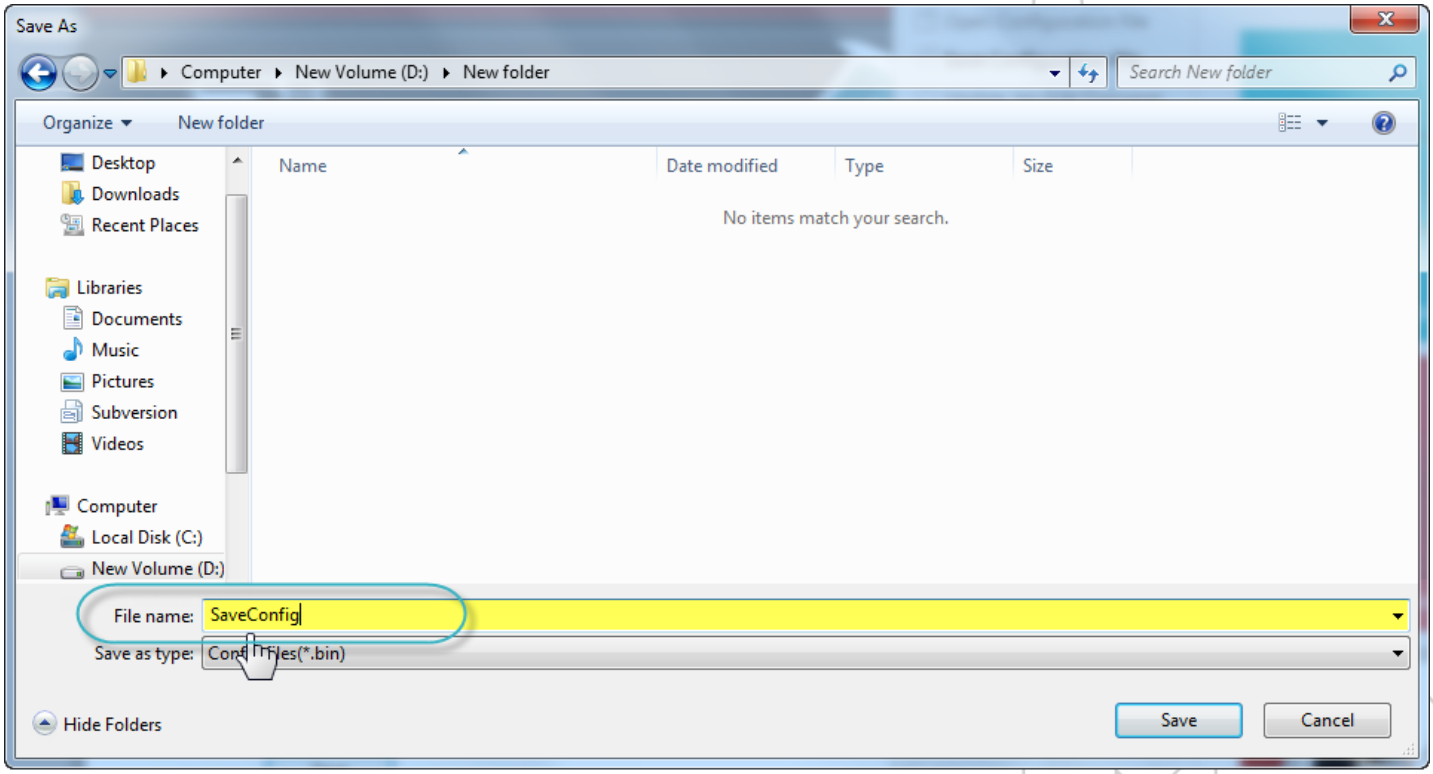
The **Save As** dialog box is displayed as shown below.



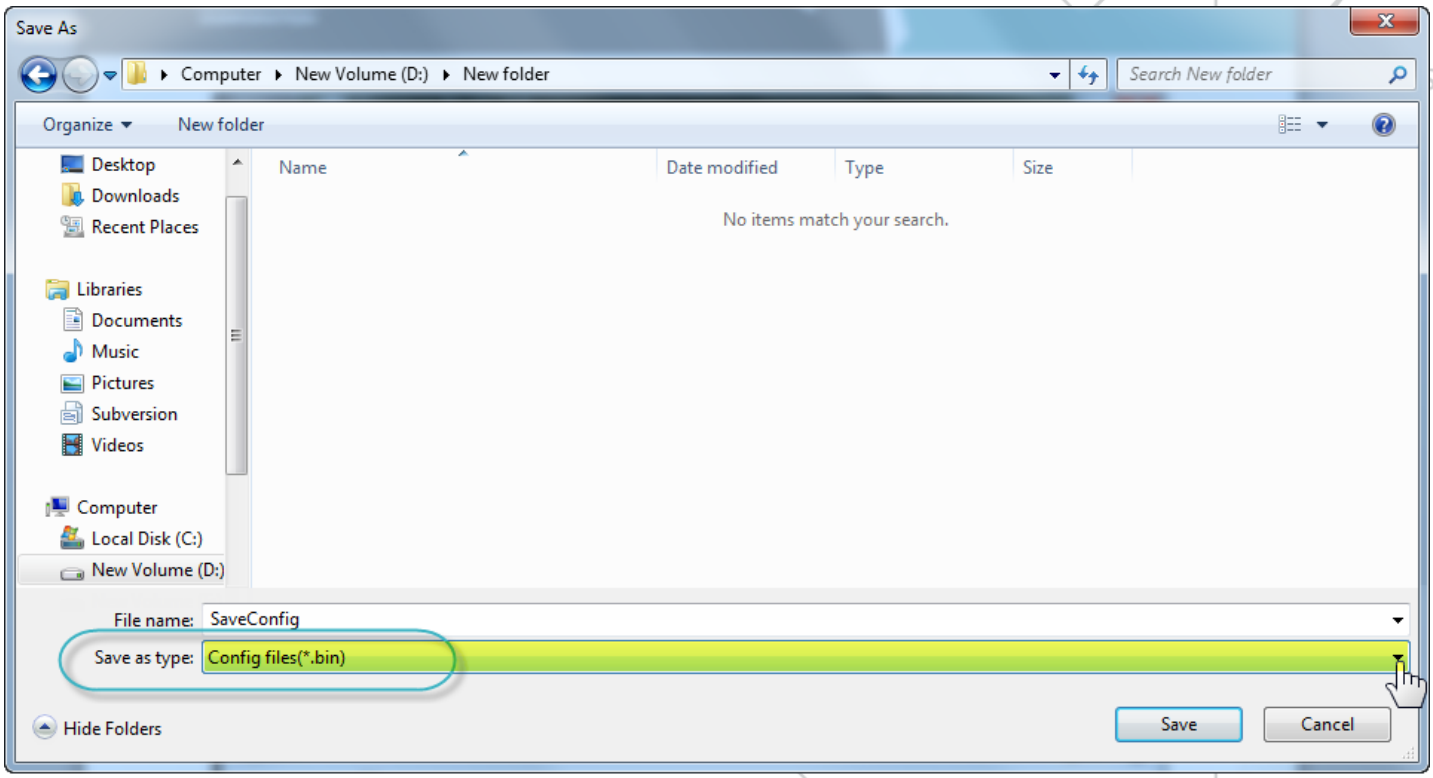
4. Select the location in your computer hard drive (C:), (D:), (F:), etc where you want to save the configuration file.



5. In the **File name** box, type-in the name of the configuration file.

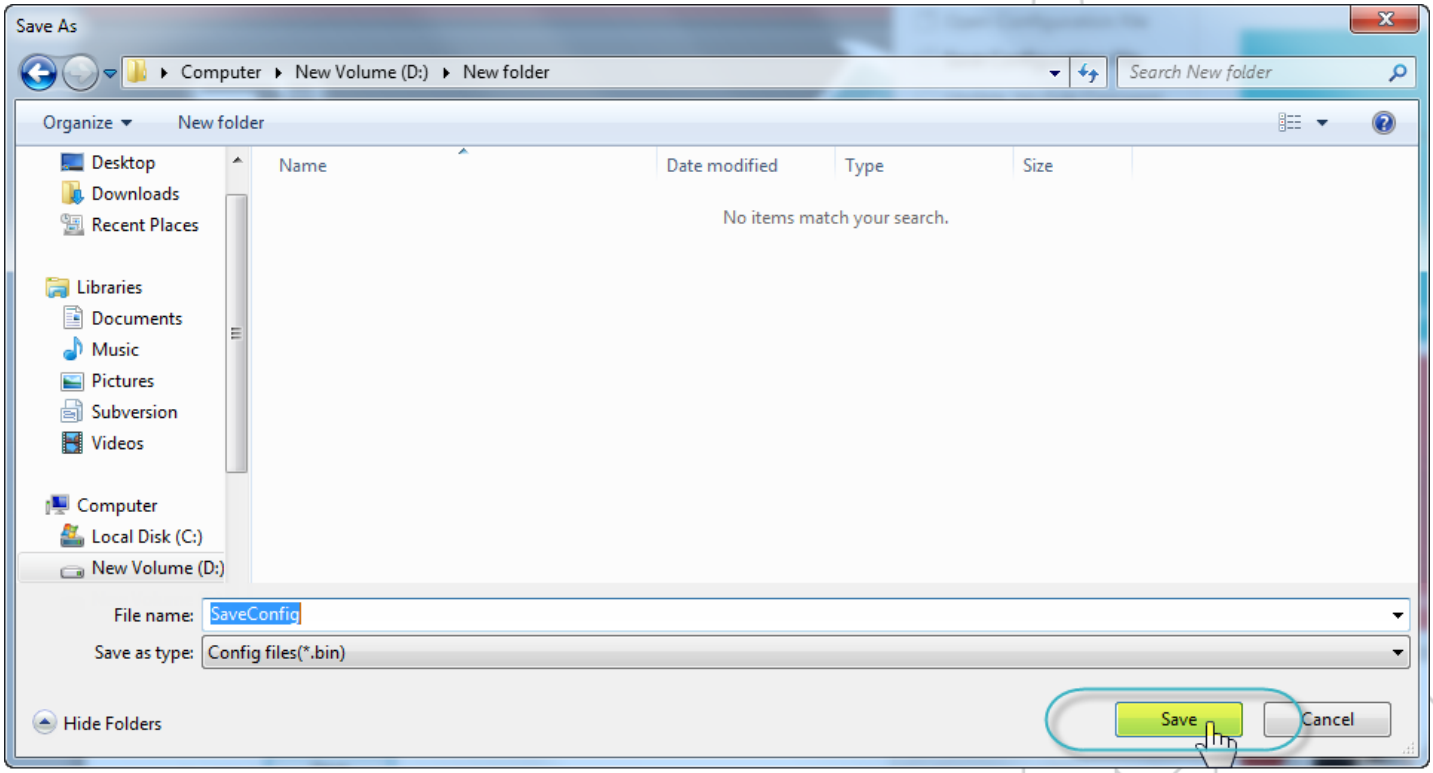


6. In the **Save as type** box, select **Config file(*.bin)** as the file type.

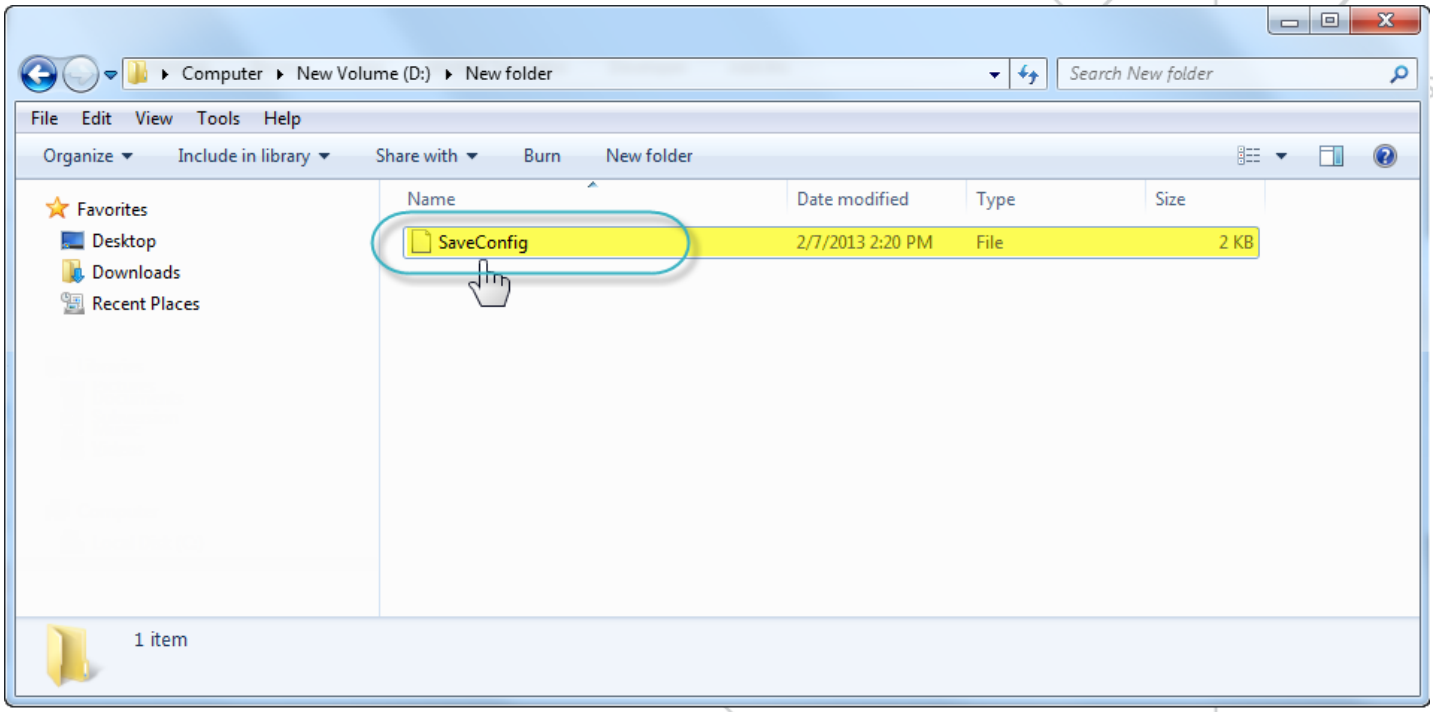


7. Click 

.



Your current configuration is saved successfully.



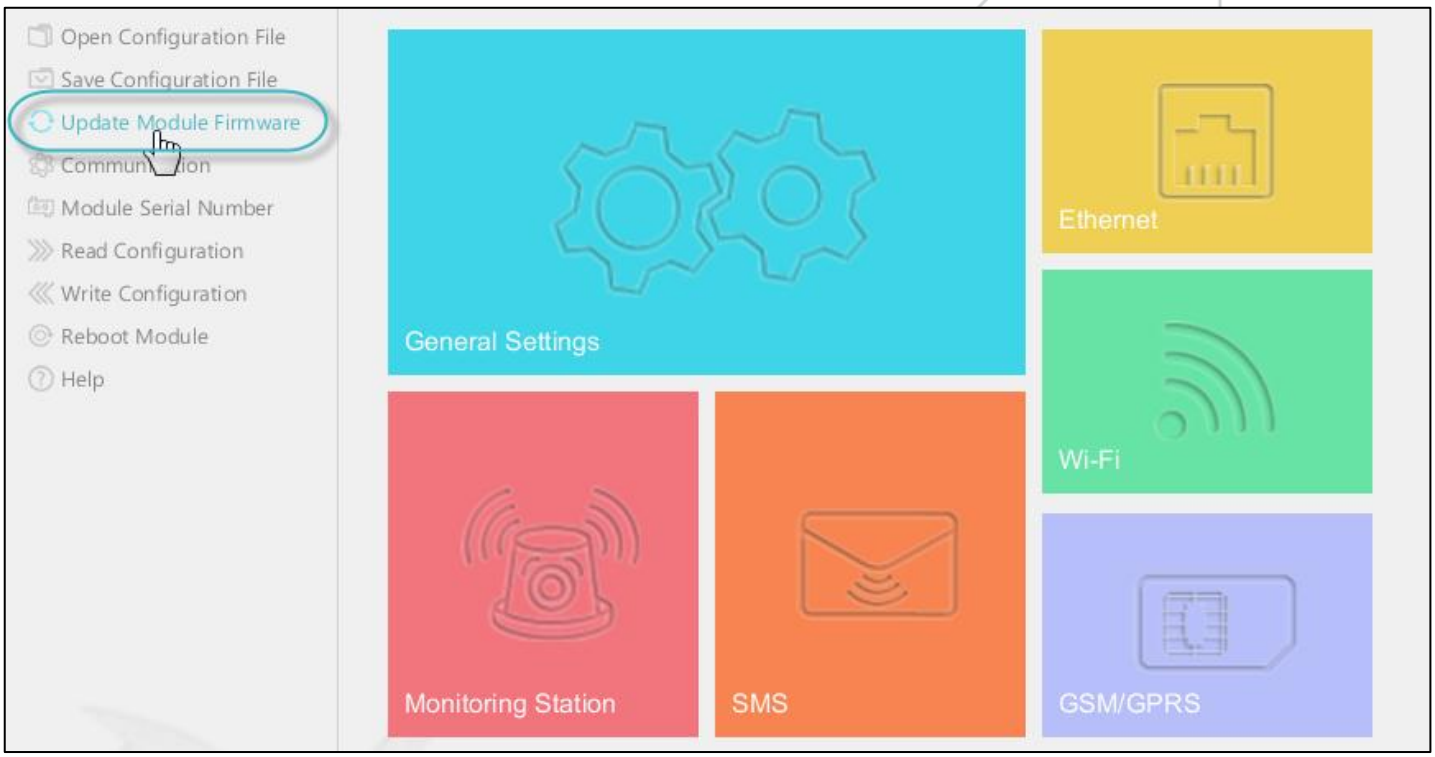
15 Update Module Firmware

The **Update Module Firmware** feature allows you to manually update Pegasus™ Modules firmware. You can import the latest firmware from your computers hard disk drive and update the modules firmware.

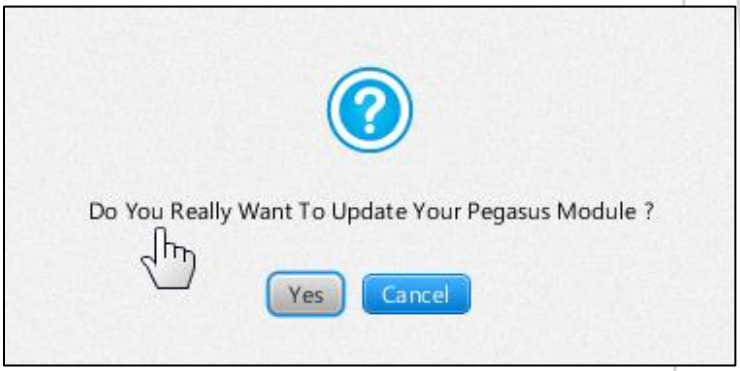
15.1. Update Your Pegasus™ Modules Firmware

To update your Pegasus™ modules firmware

1. Open the **Pegasus™ Studio Main Screen,** and then click **Update Module Firmware**.

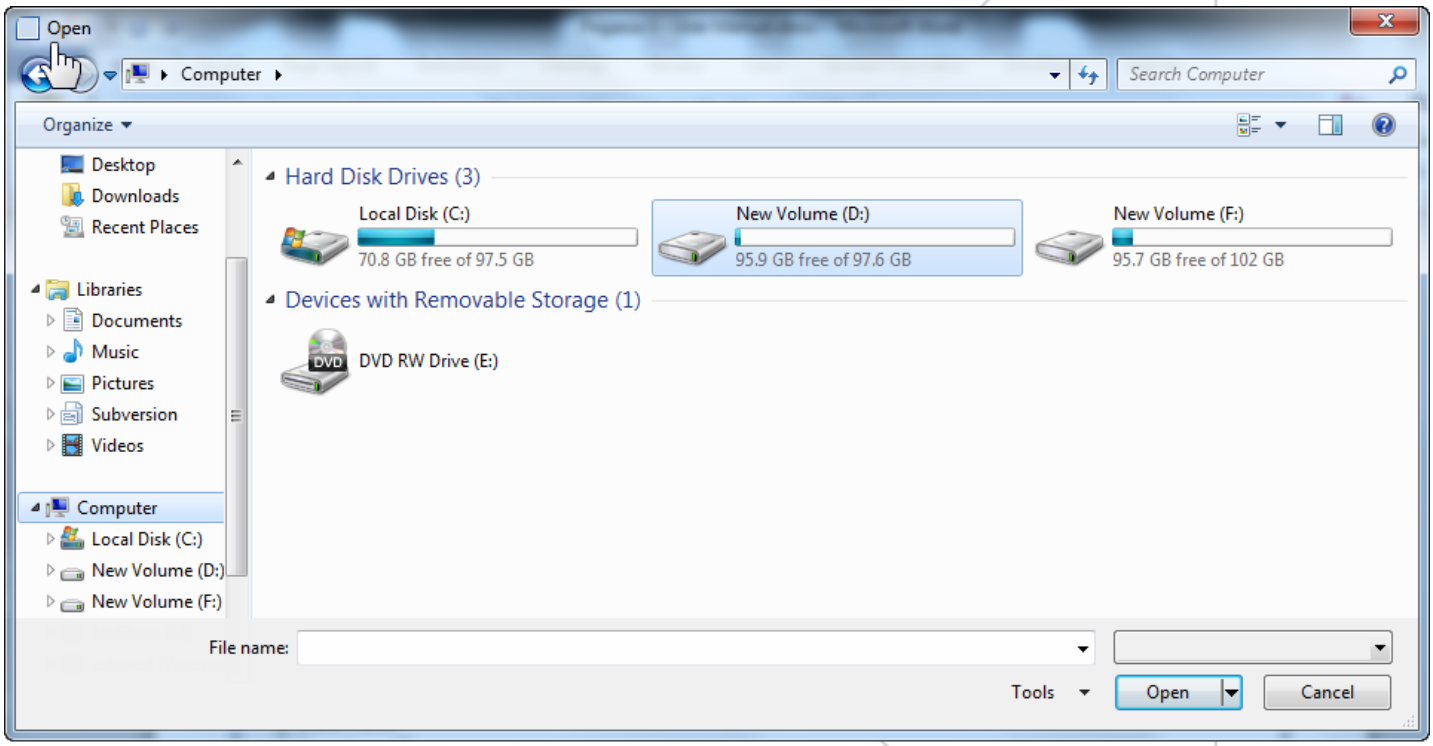


A message box saying, “Do you really want to update your Pegasus™ module?” is displayed.



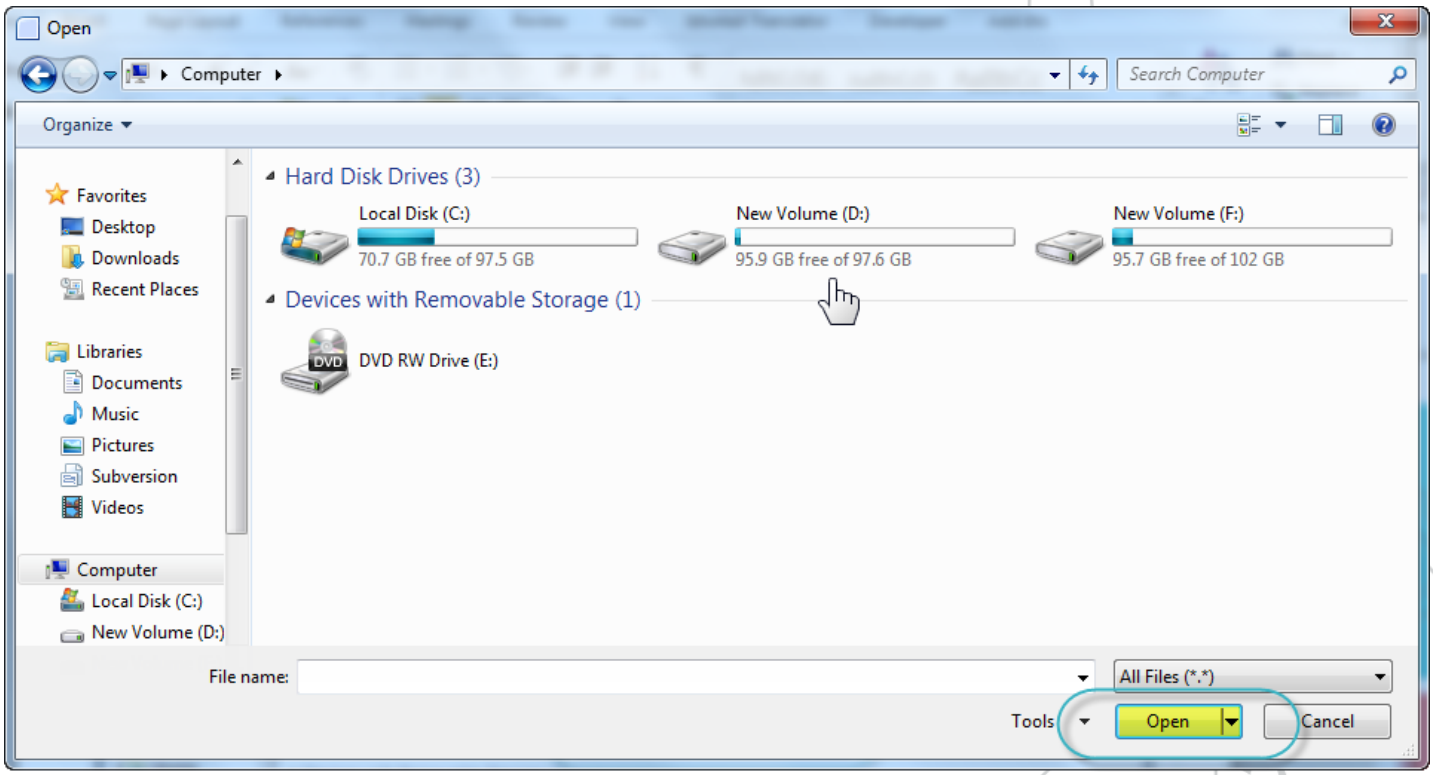
2. To proceed with the firmware update, click the **Yes** button.

The **Open** dialog box is displayed.



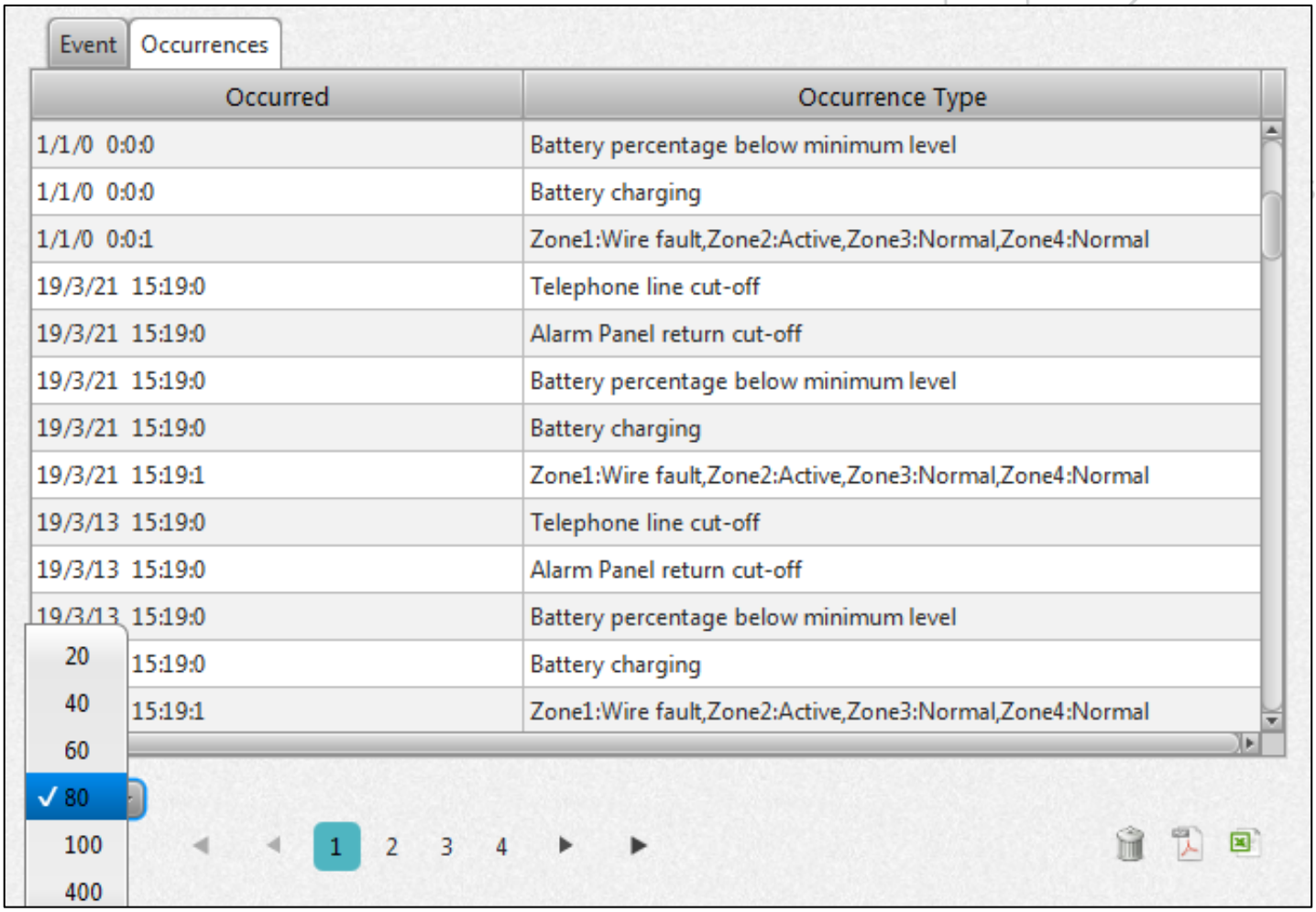
3. Browse the Firmware file from your computers hard disk drives.

4. Select the **Firmware** file, and then click the **Open** button.



16 Events/Occurrences Log

The **Events/Occurrences log** screen displays events/occurrences history/log. This screen displays upto 400 logs in a single screen to a maximum of 5000 events/occurrences. You can export the events/occurrences log to the PDF/Excel file, and save it in your computers hard disk drive. This screen allows you to delete the existing events/occurrences log.

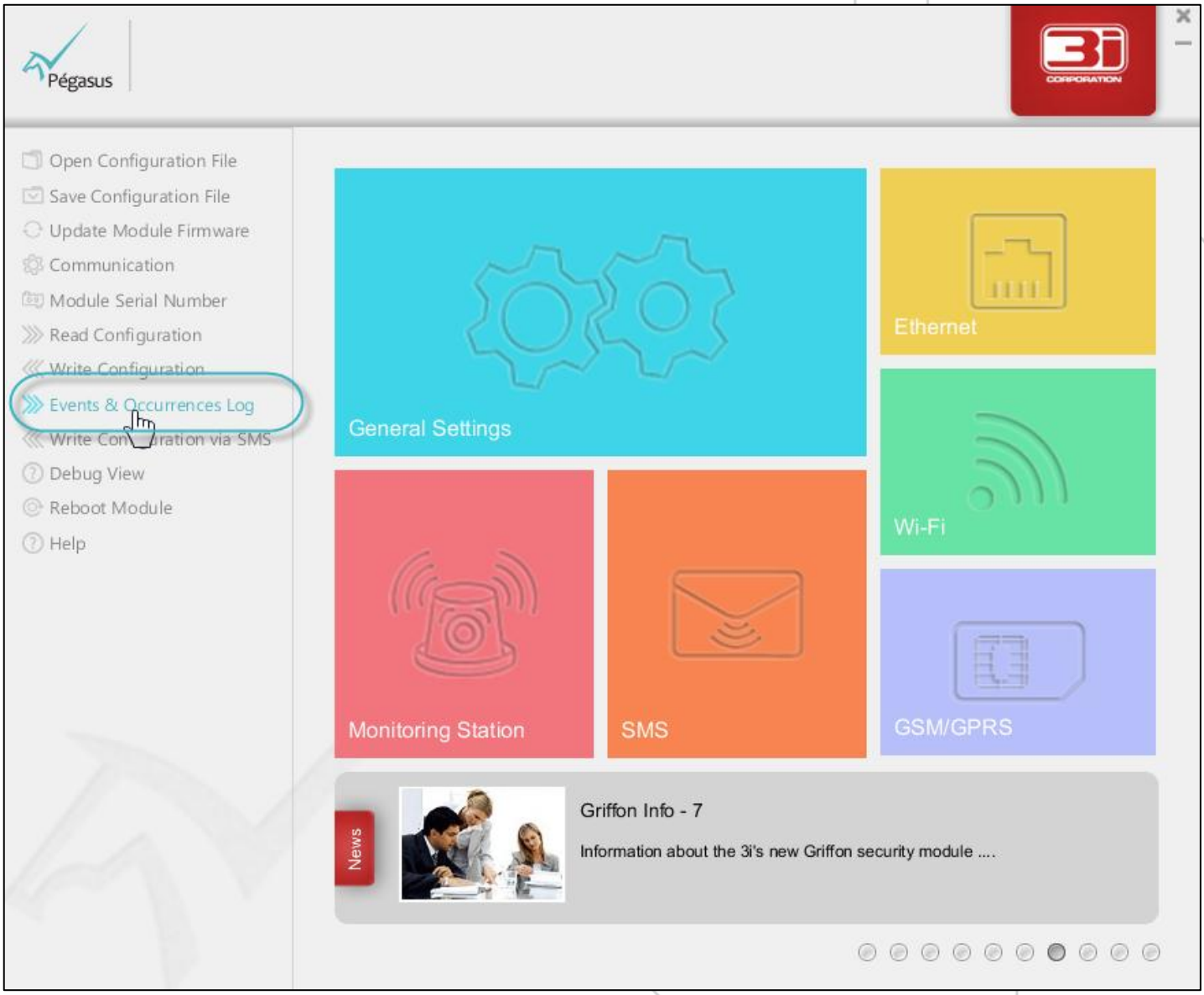


16.1. Manage Event Log

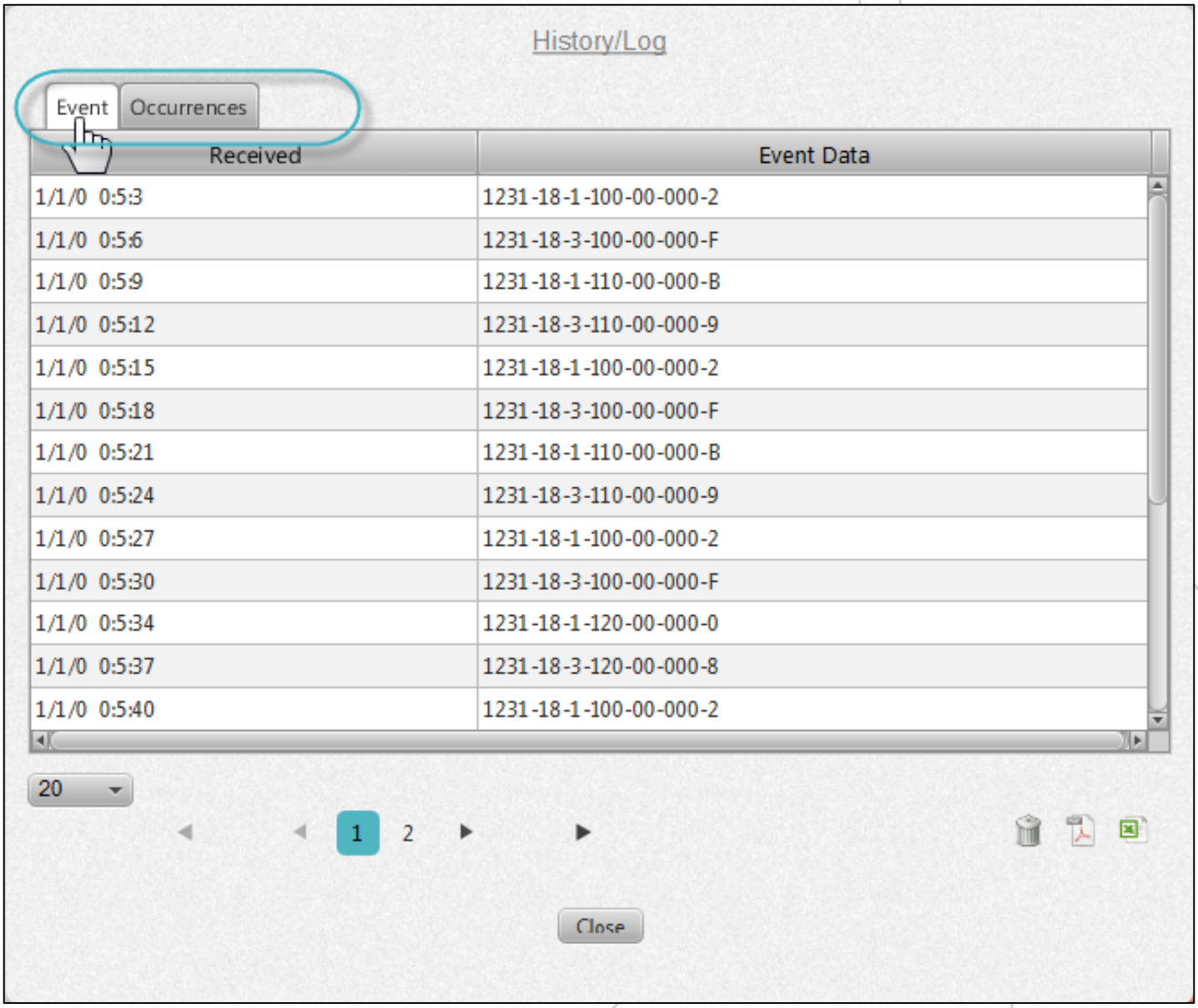
16.1.1. View Event Log

To view event log

1. On the **Pegasus™ Studio** menu, click **Events & Occurrences Log**.

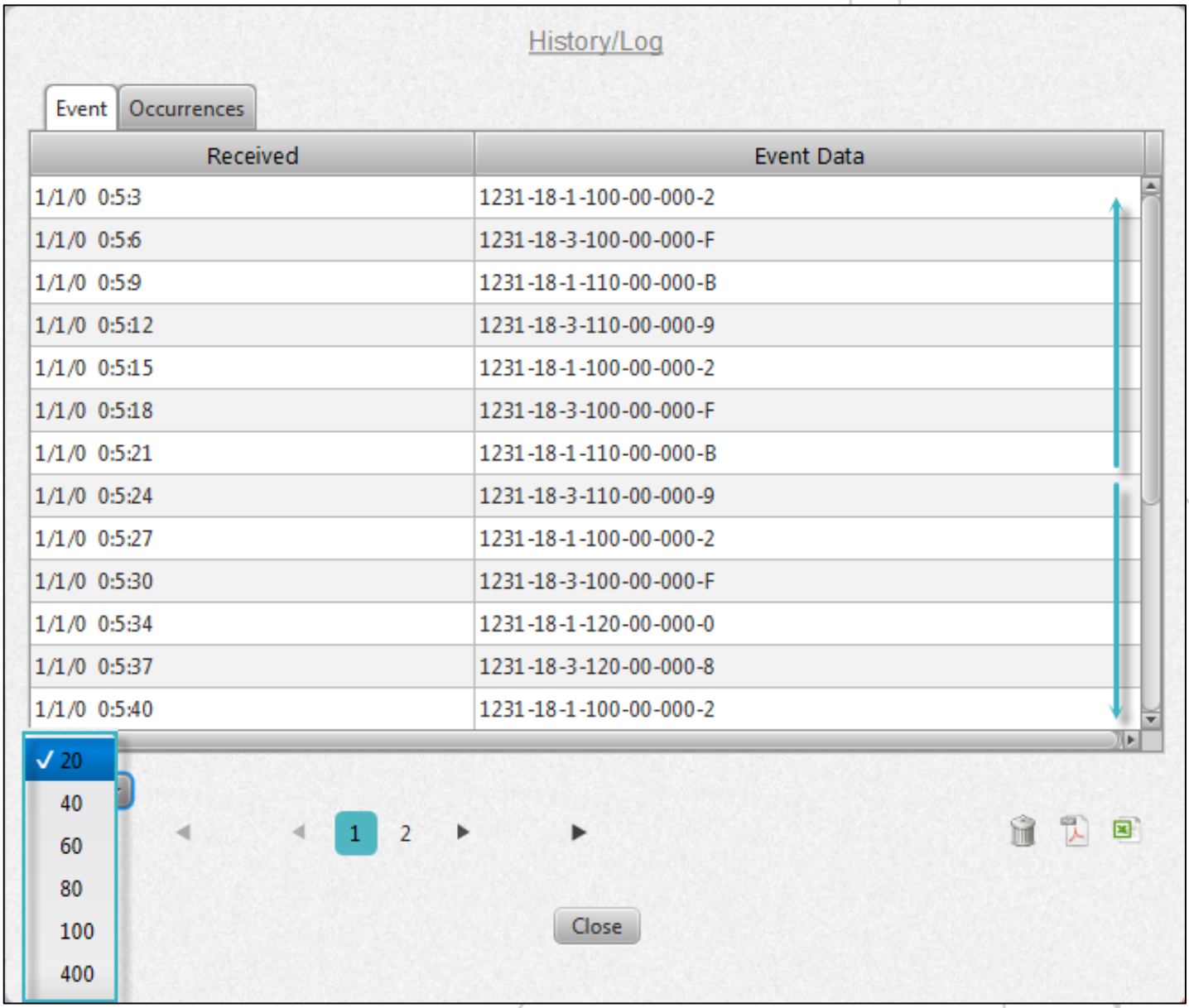


2. The **History/Log** dialog box is displayed. Click the **Event** tab as shown in the below image. All events with the received date and time, and event data are displayed.



3. You can customize the event log view. Click the drop-down arrow as shown in the below image.

4. Select the event log view as **20/40/60/80/100/400** per page. Use the scroll bar to view all events in ascending order.

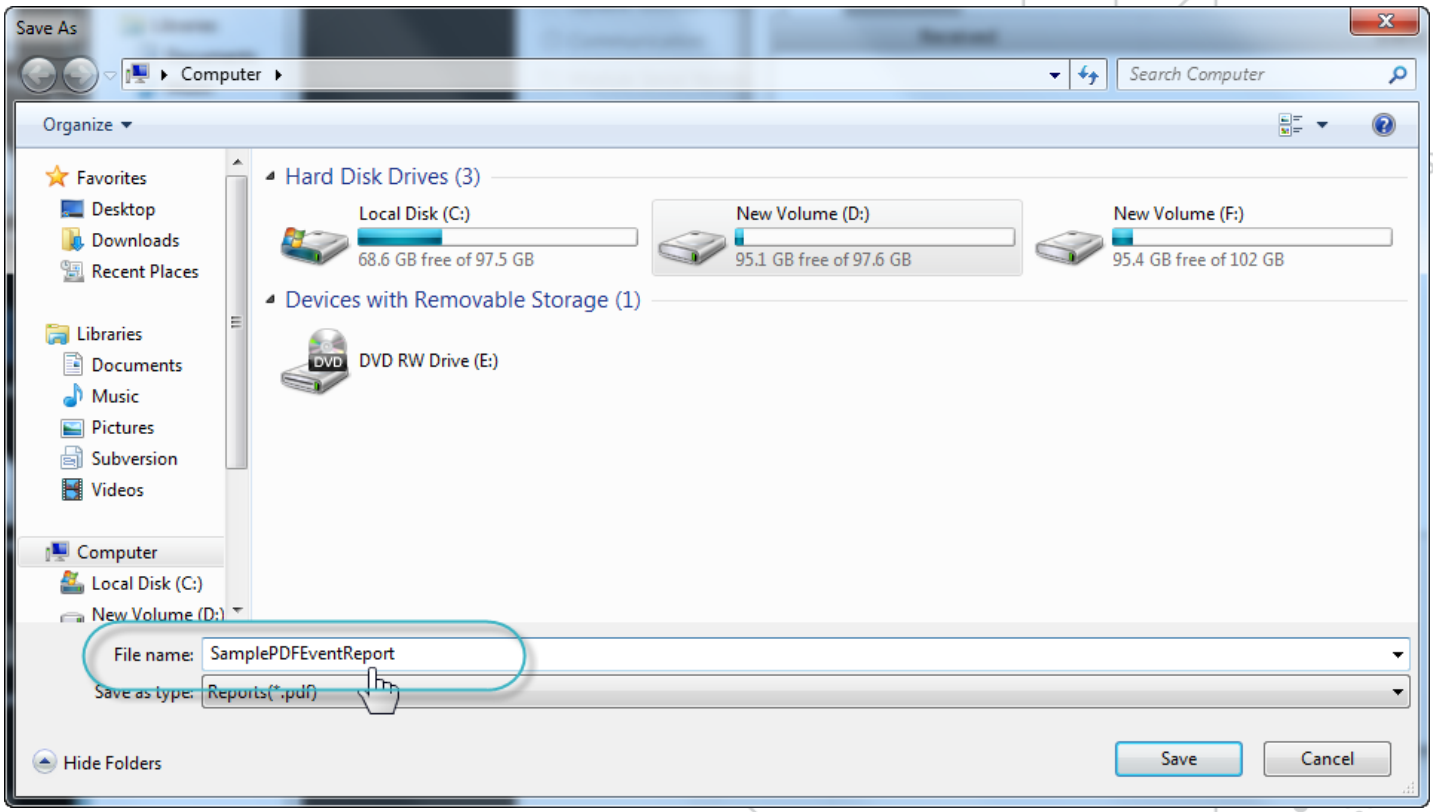


16.1.2. Generate Event Logs in PDF

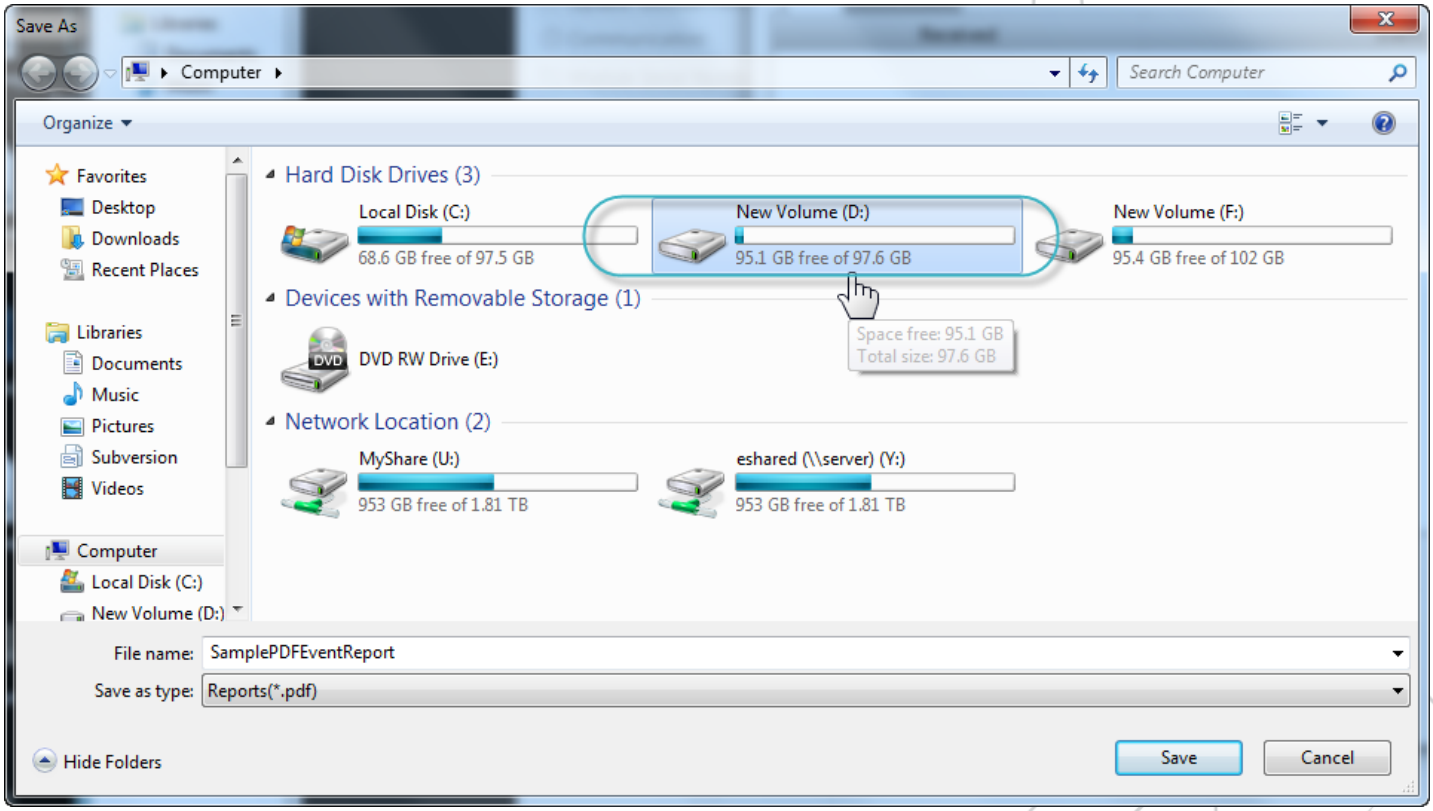
To generate event logs in pdf

1. Click the **Export PDF**  icon..

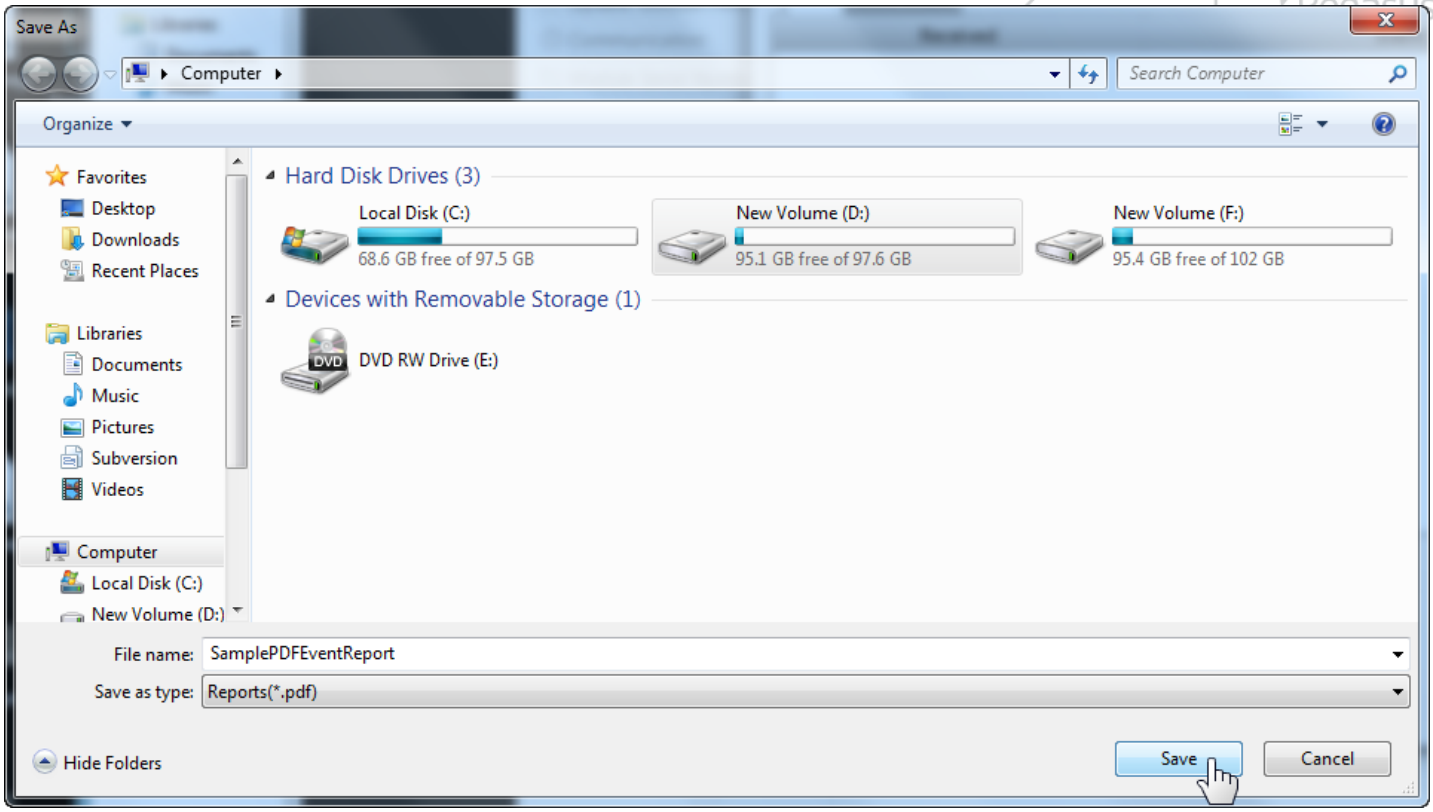
2. The **Save As** dialog box is displayed. In the **File Name** drop-down box, type-in the pdf name.



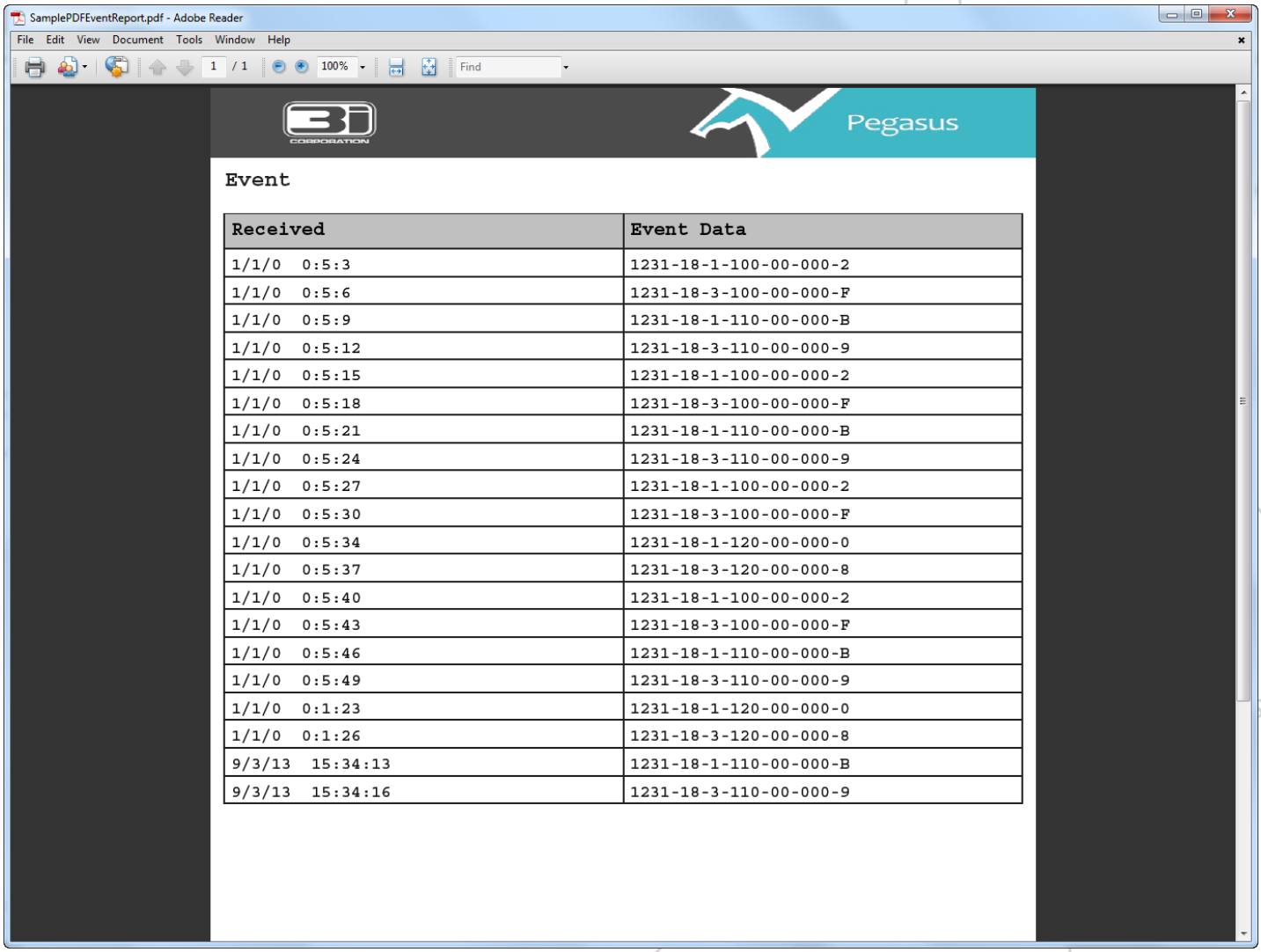
3. Select a location in your hard disk drive where you want to save the pdf file.



4. Click the **Save** button.



The Event logs in PDF are generated and saved in the specified location in your hard drive. A sample Event logs PDF is shown below.



Event

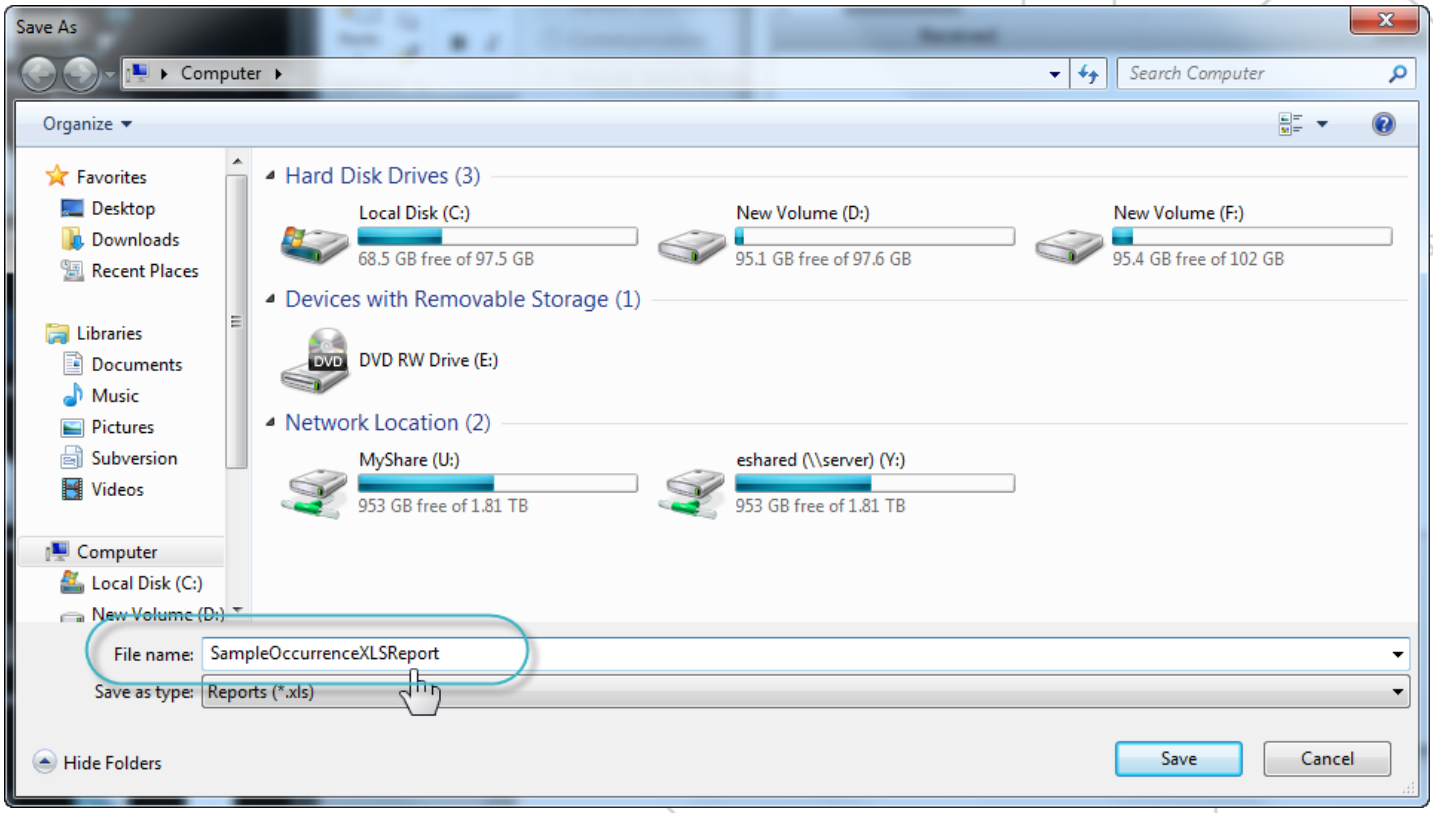
Received	Event Data
1/1/0 0:5:3	1231-18-1-100-00-000-2
1/1/0 0:5:6	1231-18-3-100-00-000-F
1/1/0 0:5:9	1231-18-1-110-00-000-B
1/1/0 0:5:12	1231-18-3-110-00-000-9
1/1/0 0:5:15	1231-18-1-100-00-000-2
1/1/0 0:5:18	1231-18-3-100-00-000-F
1/1/0 0:5:21	1231-18-1-110-00-000-B
1/1/0 0:5:24	1231-18-3-110-00-000-9
1/1/0 0:5:27	1231-18-1-100-00-000-2
1/1/0 0:5:30	1231-18-3-100-00-000-F
1/1/0 0:5:34	1231-18-1-120-00-000-0
1/1/0 0:5:37	1231-18-3-120-00-000-8
1/1/0 0:5:40	1231-18-1-100-00-000-2
1/1/0 0:5:43	1231-18-3-100-00-000-F
1/1/0 0:5:46	1231-18-1-110-00-000-B
1/1/0 0:5:49	1231-18-3-110-00-000-9
1/1/0 0:1:23	1231-18-1-120-00-000-0
1/1/0 0:1:26	1231-18-3-120-00-000-8
9/3/13 15:34:13	1231-18-1-110-00-000-B
9/3/13 15:34:16	1231-18-3-110-00-000-9

16.1.3. Generate Event Logs in the Excel Format

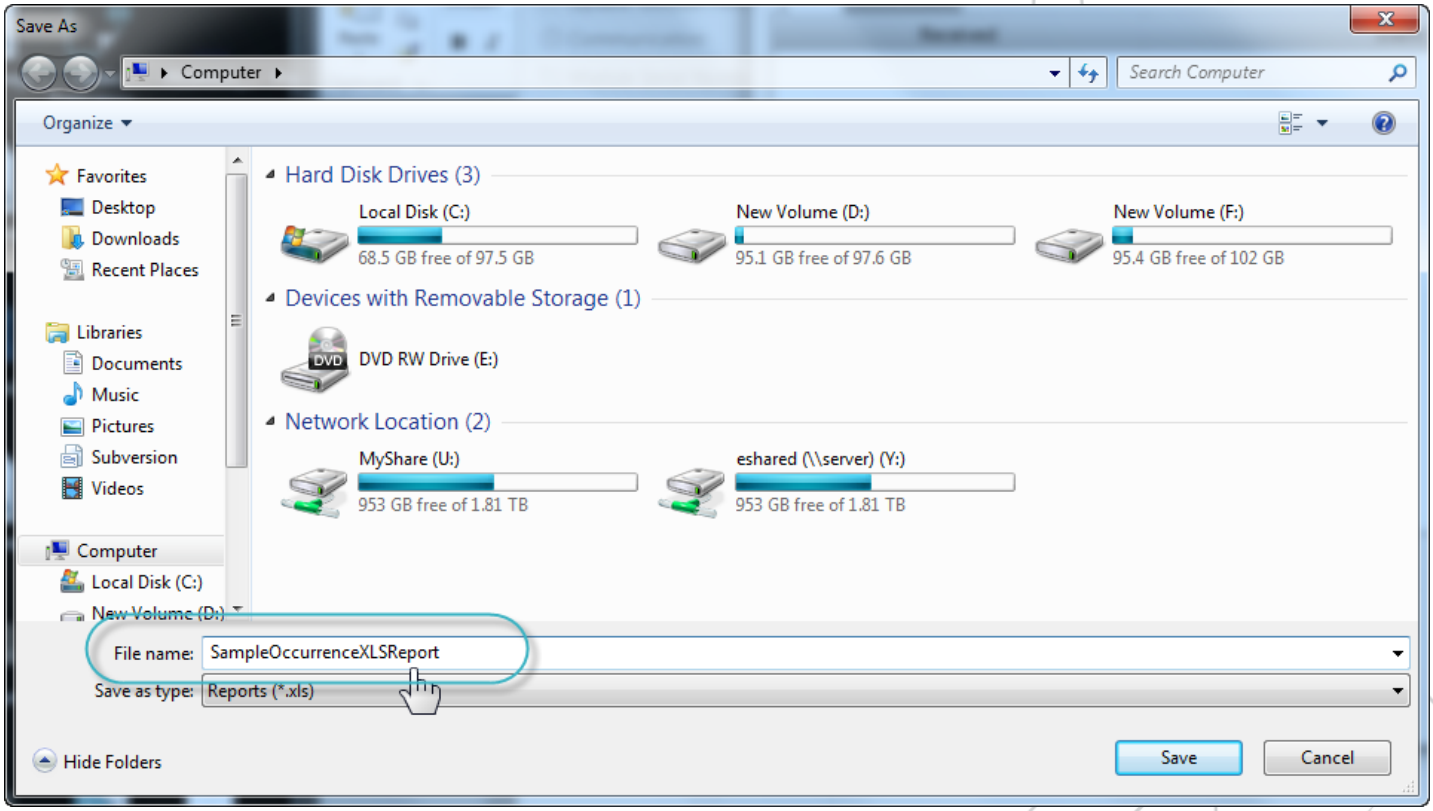
To generate event logs in the Excel format

1. Click the **Export Excel**  icon.

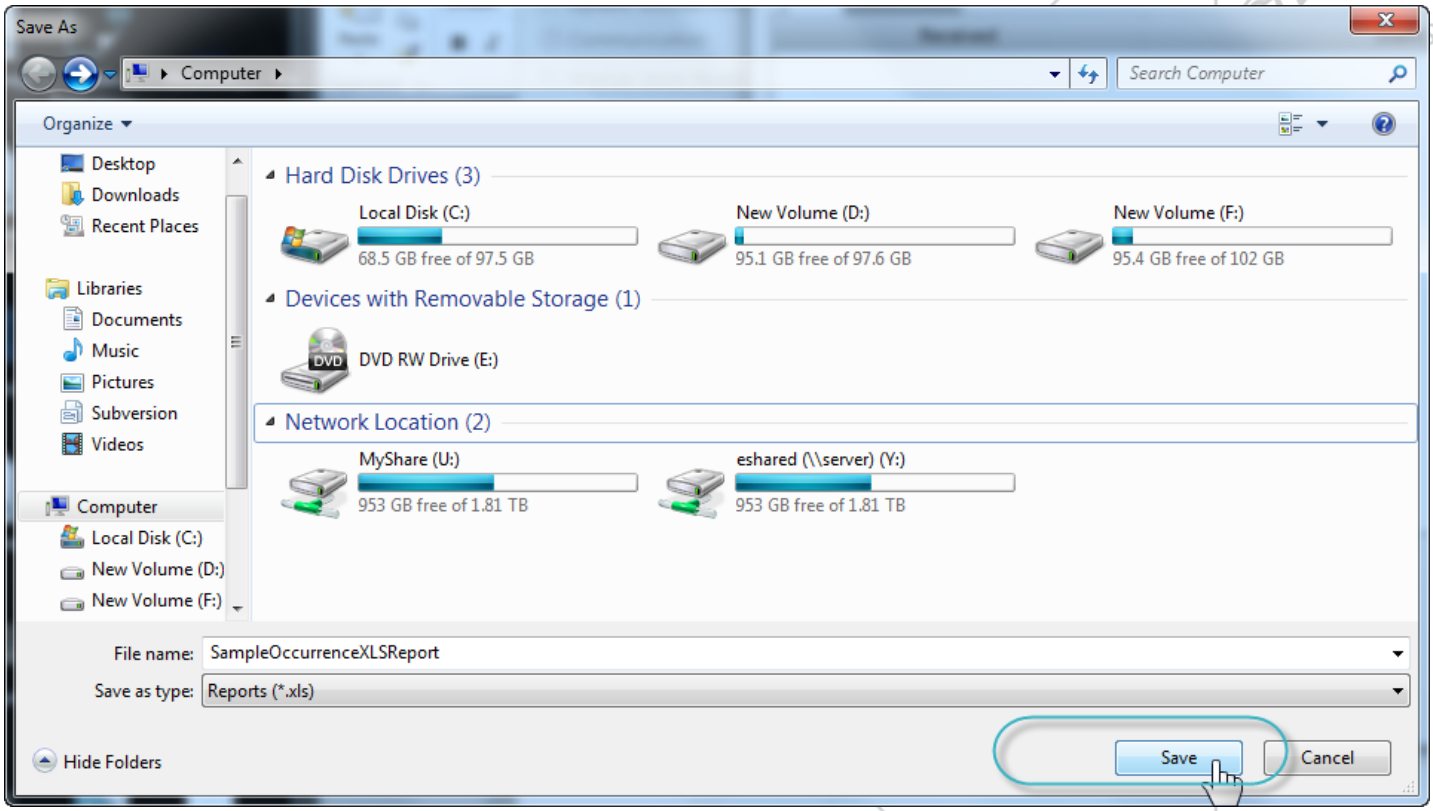
2. The **Save As** dialog box is displayed. In the **File Name** drop-down box, type-in the Excel file name.



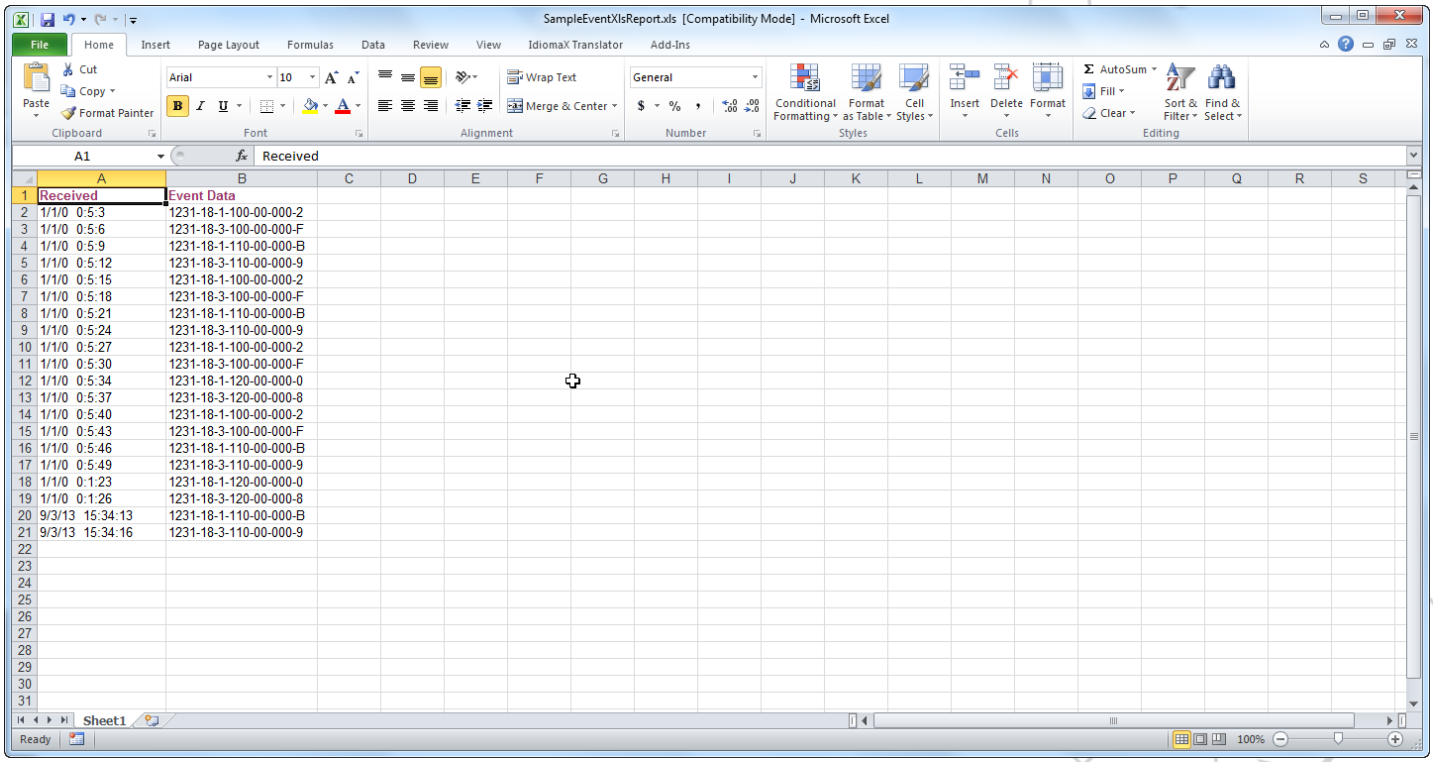
3. Select a location in your hard disk drive where you want to save the Excel file.



4. Click the **Save** button.



The Event logs in the Excel format are generated and saved in the specified location in your hard drive. A sample Event logs Excel file is shown below.

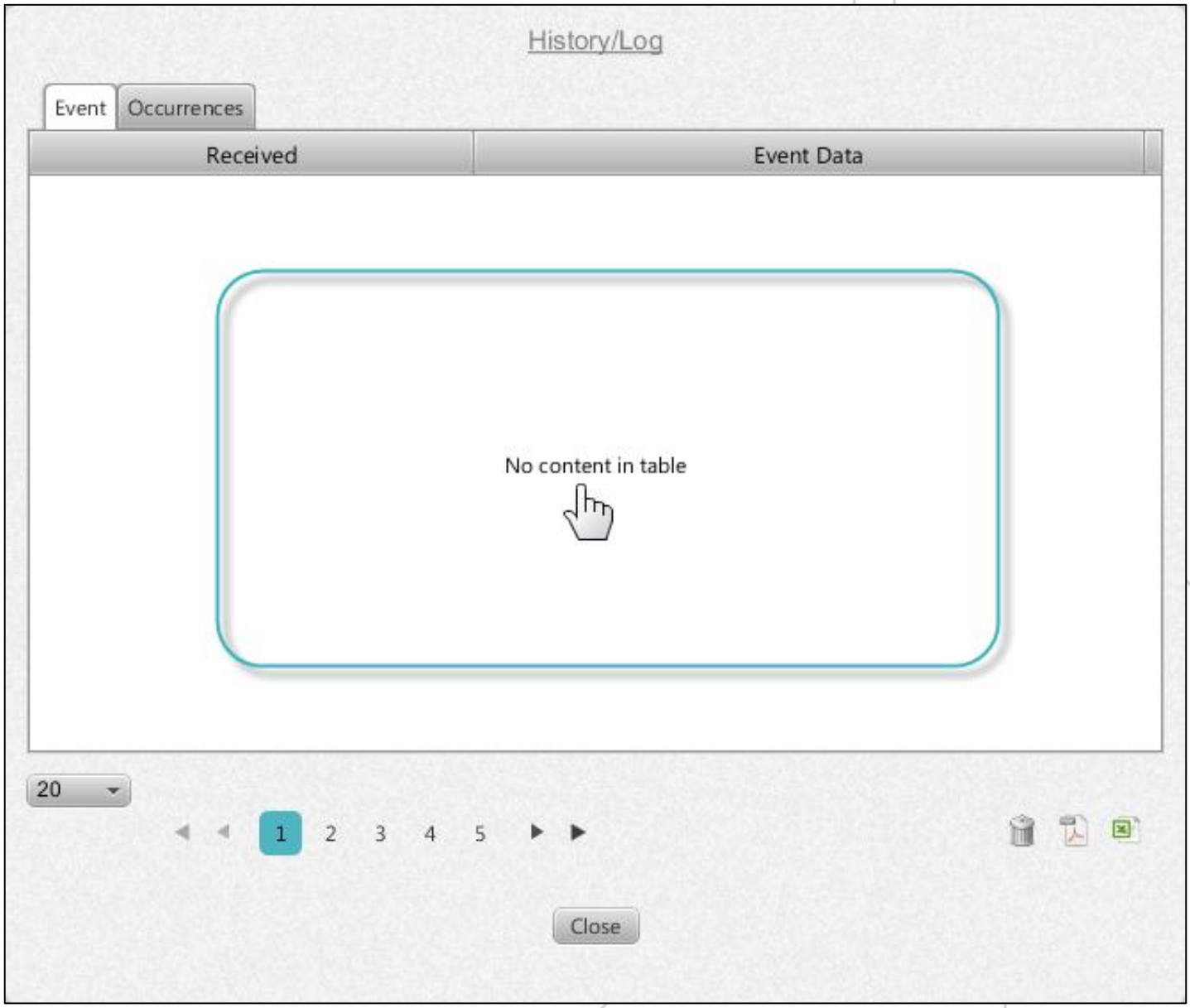


16.1.4. Delete Event Logs

To delete event logs

1. Click the **Delete**  icon.

All the Event logs are deleted.

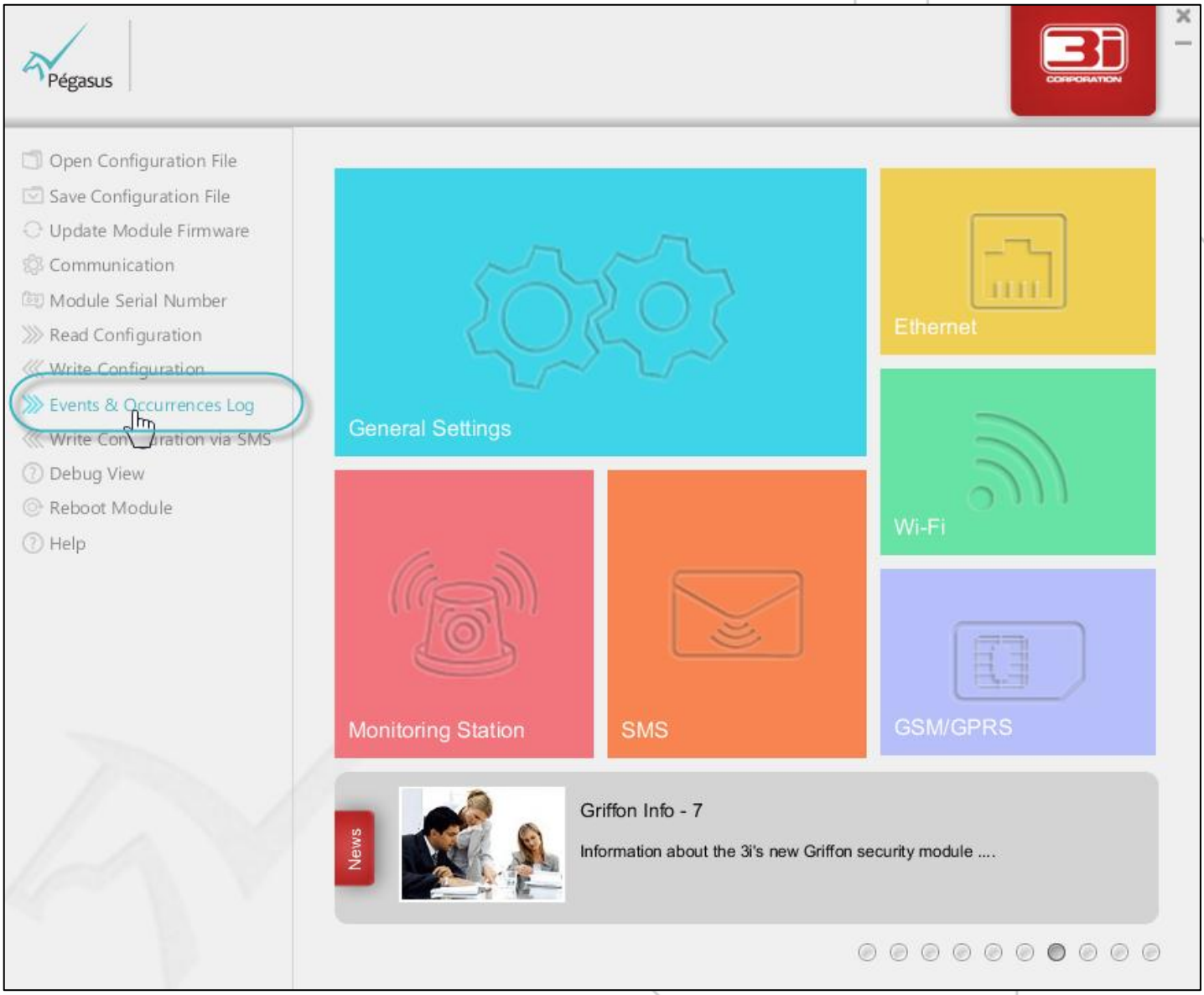

History/Log
Event
Occurrences
Received
Event Data
No content in table
20
1
2
3
4
5
Close

16.2. Manage Occurrence Logs

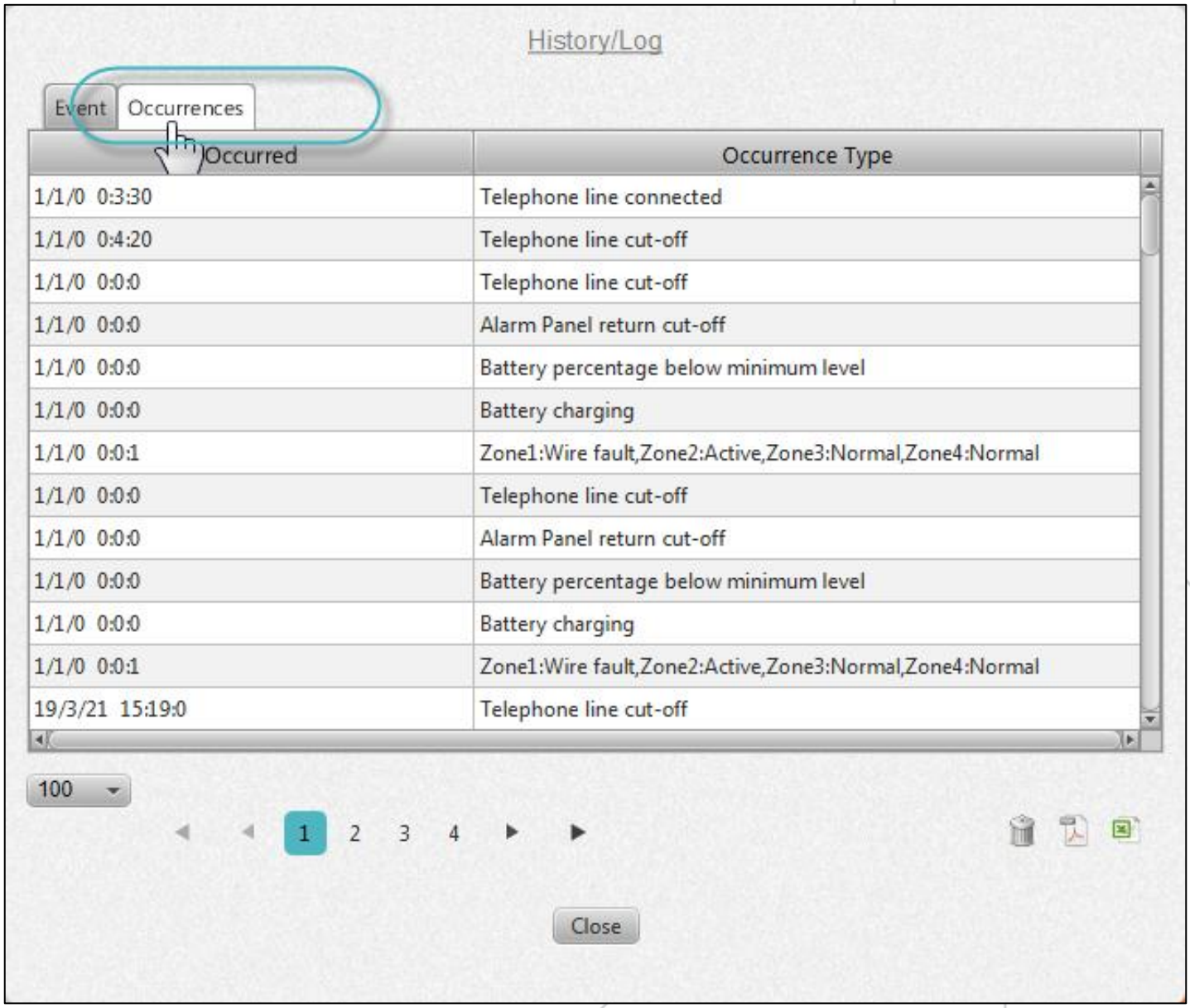
16.2.1. View Occurrence Logs

To view occurrence logs

1. On the **Pegasus™ Studio** menu, click **Events & Occurrences Log**.

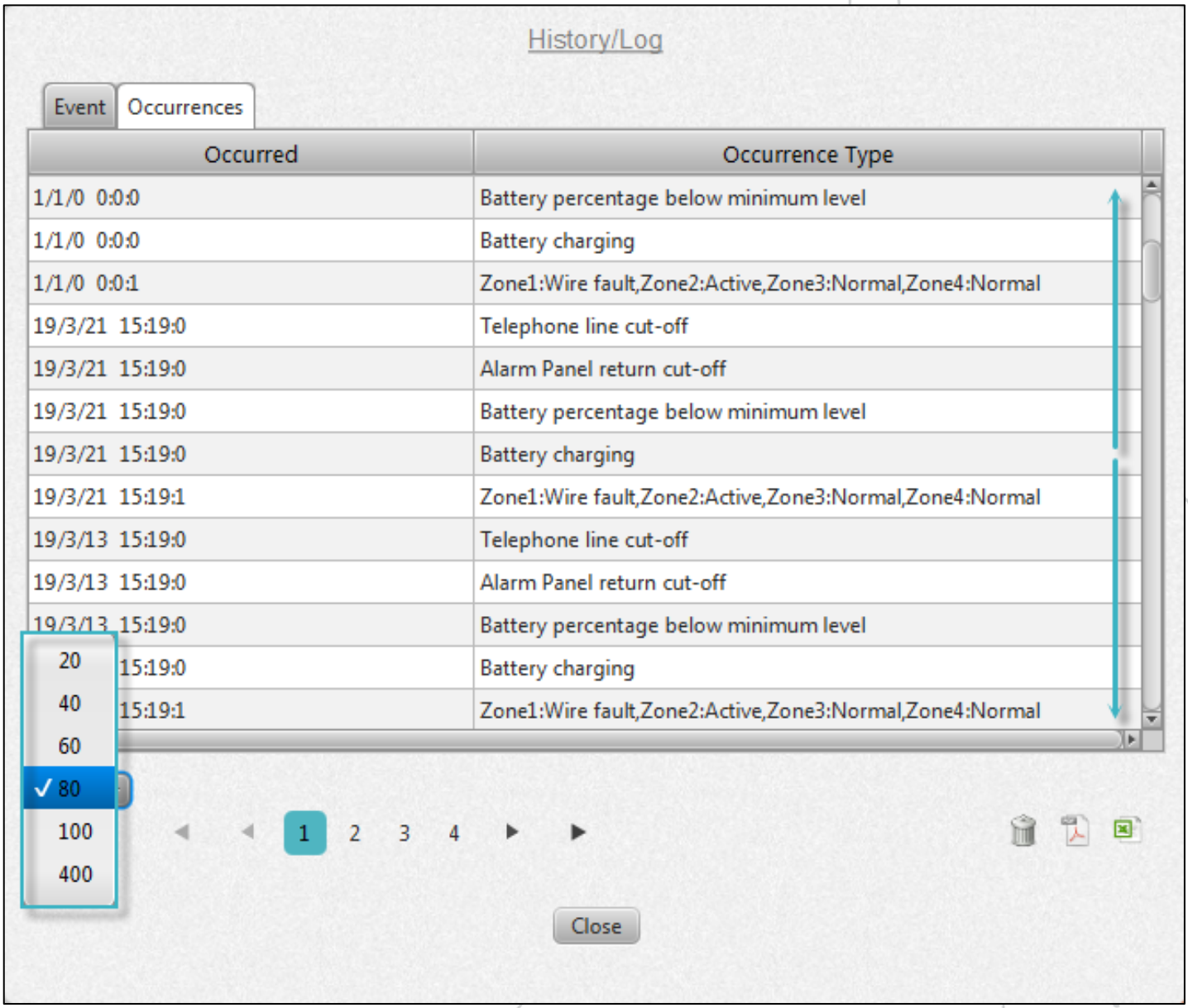


2. The **History/Log** dialog box is displayed. Click the **Occurrence** tab as shown in the below image. All occurrences with the received date and time, and event data are displayed.



3. You can customize the occurrence log view. Click the drop-down arrow as shown in the below image.

4. Select the event log view as **20/40/60/80/100/400** per page. Use the scroll bar to view all events in ascending order.

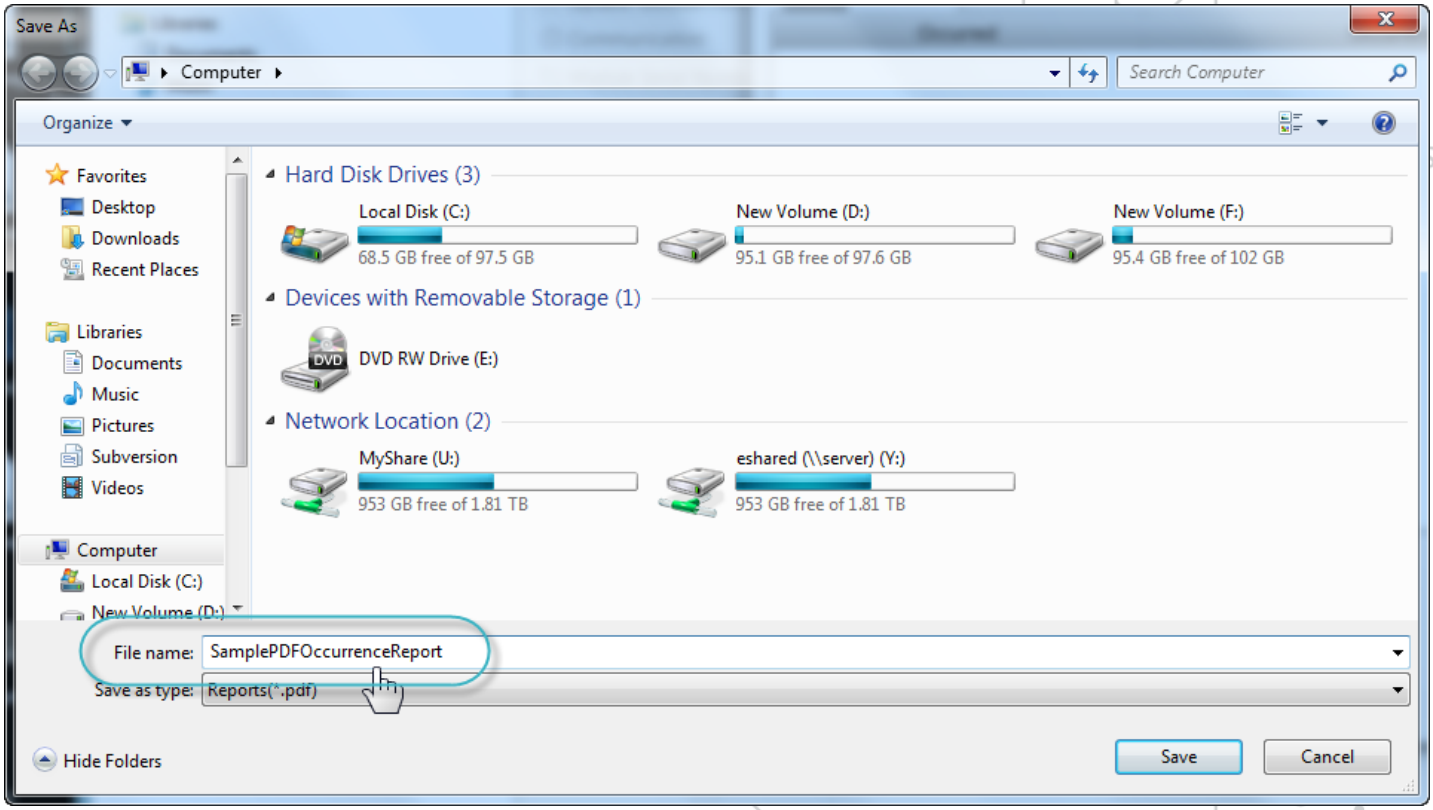


16.2.2. Generate Event Logs in PDF

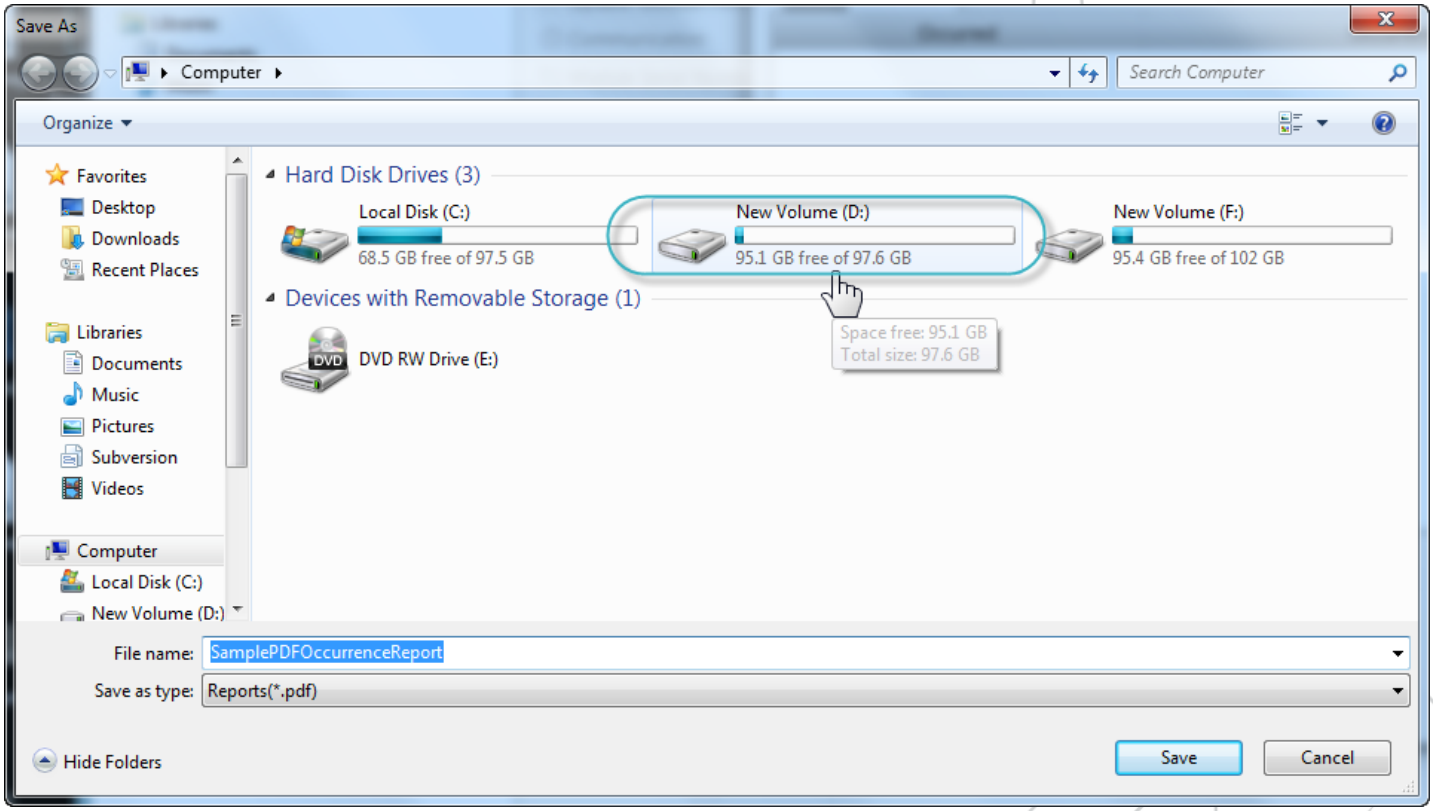
To generate event logs in pdf

5. Click the **Export PDF** icon.

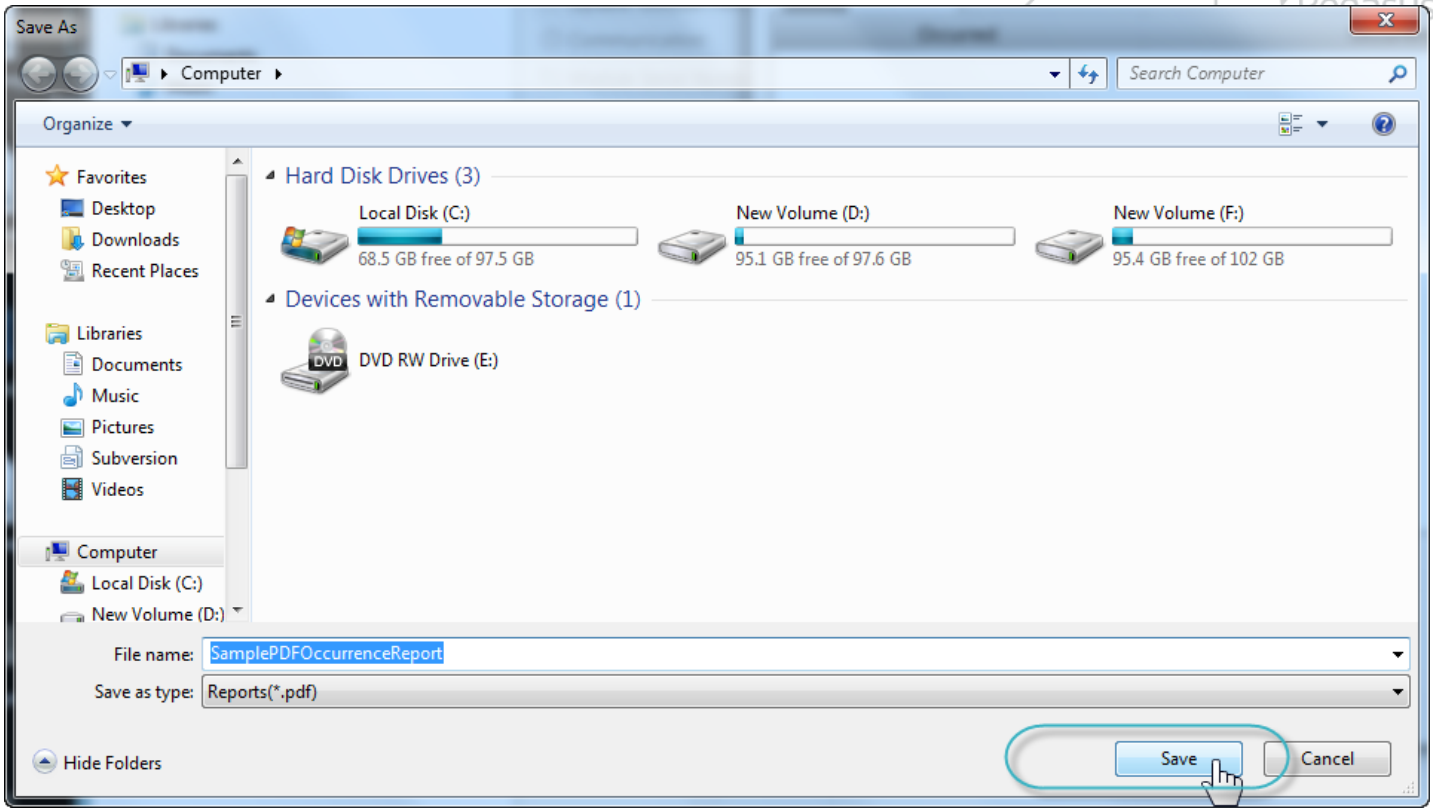
6. The **Save As** dialog box is displayed. In the **File Name** drop-down box, type-in the pdf name.



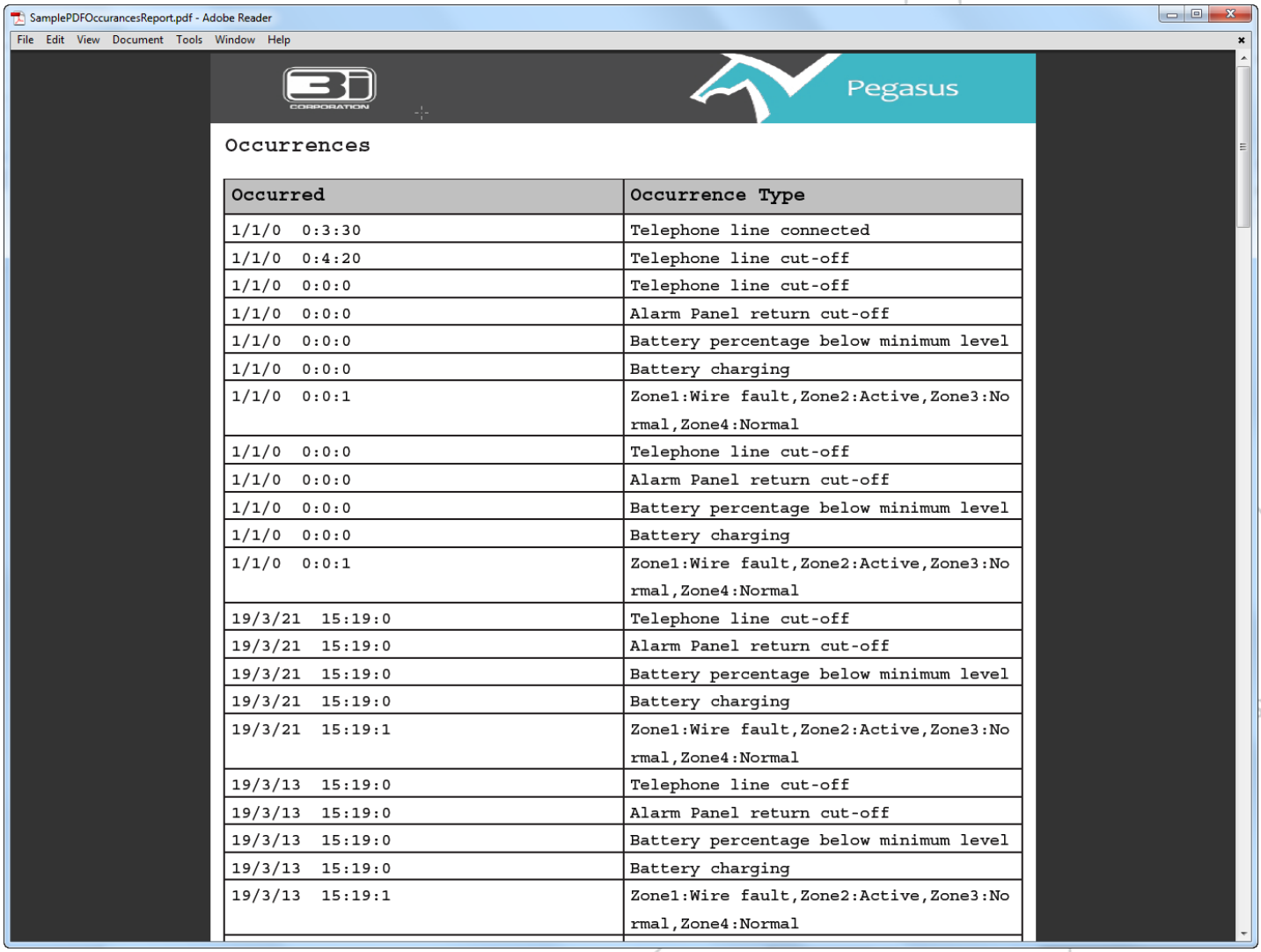
7. Select a location in your hard disk drive where you want to save the pdf file.



8. Click the **Save** button.



The Event logs in PDF are generated and saved in the specified location in your hard drive. A sample Event logs PDF is shown below.



SamplePDFOccurancesReport.pdf - Adobe Reader

File Edit View Document Tools Window Help

Pegasus

Occurrences

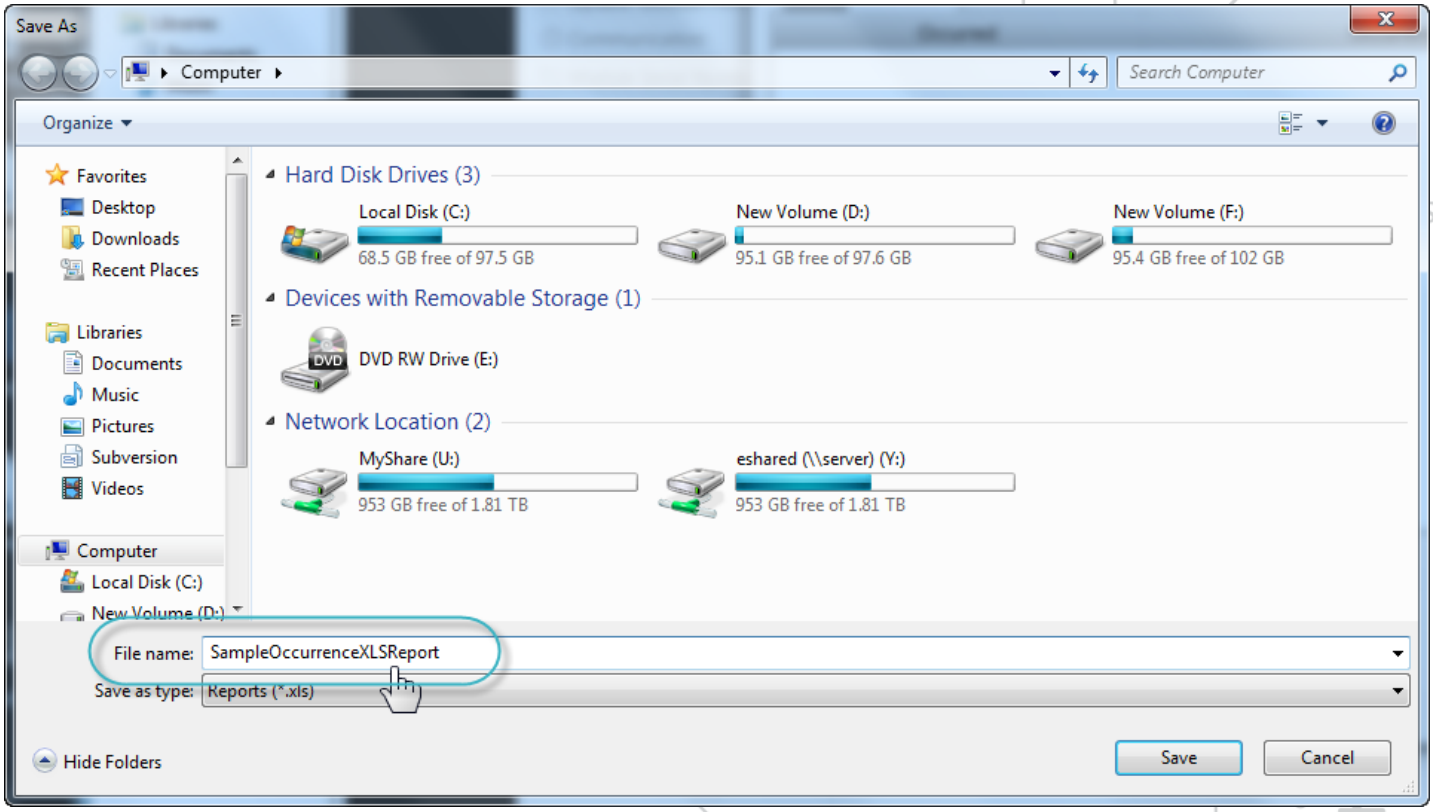
Occurred	Occurrence Type
1/1/0 0:3:30	Telephone line connected
1/1/0 0:4:20	Telephone line cut-off
1/1/0 0:0:0	Telephone line cut-off
1/1/0 0:0:0	Alarm Panel return cut-off
1/1/0 0:0:0	Battery percentage below minimum level
1/1/0 0:0:0	Battery charging
1/1/0 0:0:1	Zone1:Wire fault,Zone2:Active,Zone3:Normal,Zone4:Normal
1/1/0 0:0:0	Telephone line cut-off
1/1/0 0:0:0	Alarm Panel return cut-off
1/1/0 0:0:0	Battery percentage below minimum level
1/1/0 0:0:0	Battery charging
1/1/0 0:0:1	Zone1:Wire fault,Zone2:Active,Zone3:Normal,Zone4:Normal
19/3/21 15:19:0	Telephone line cut-off
19/3/21 15:19:0	Alarm Panel return cut-off
19/3/21 15:19:0	Battery percentage below minimum level
19/3/21 15:19:0	Battery charging
19/3/21 15:19:1	Zone1:Wire fault,Zone2:Active,Zone3:Normal,Zone4:Normal
19/3/13 15:19:0	Telephone line cut-off
19/3/13 15:19:0	Alarm Panel return cut-off
19/3/13 15:19:0	Battery percentage below minimum level
19/3/13 15:19:0	Battery charging
19/3/13 15:19:1	Zone1:Wire fault,Zone2:Active,Zone3:Normal,Zone4:Normal

16.2.3. Generate Event Logs in Excel Format

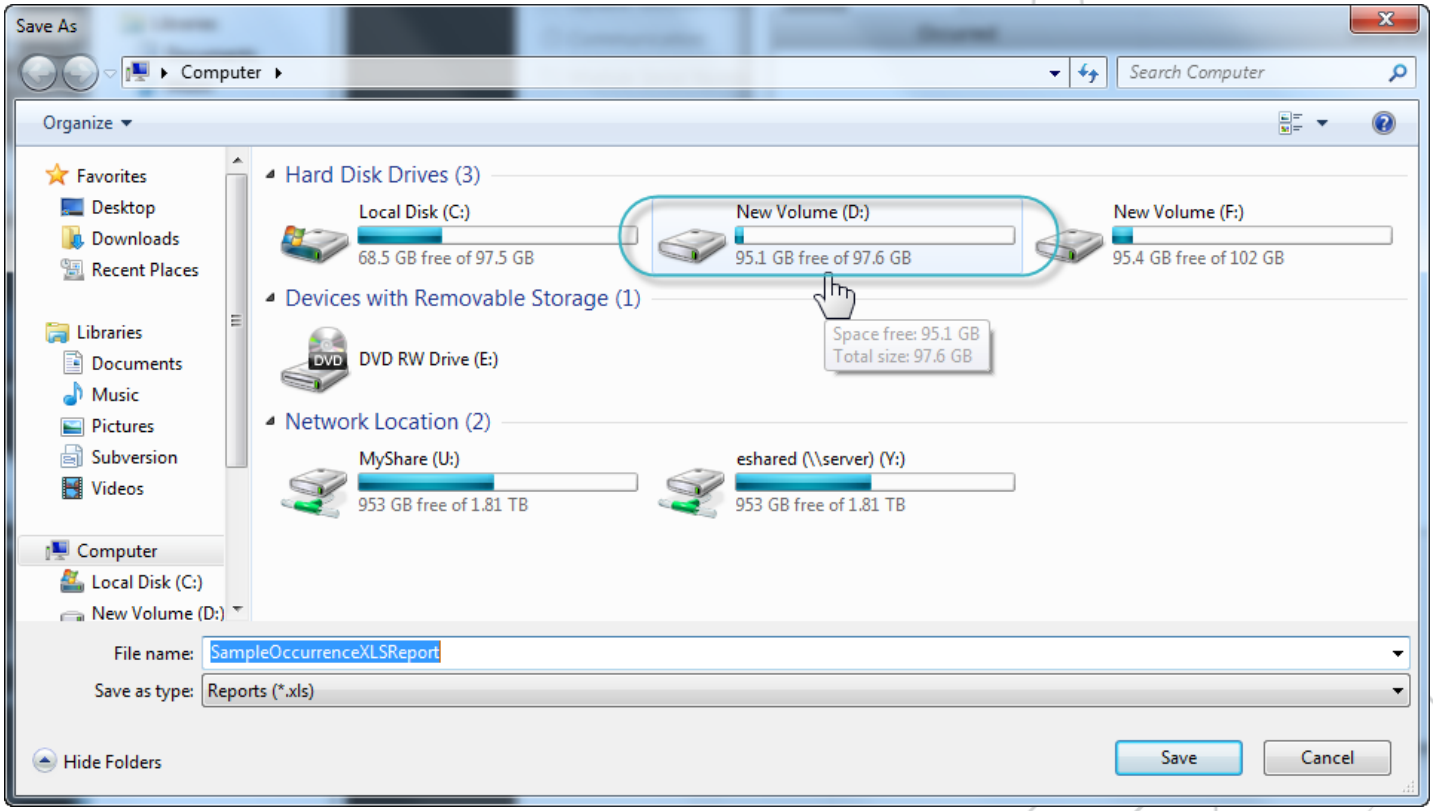
To generate event logs in Excel format

1. Click the **Export Excel**  icon.

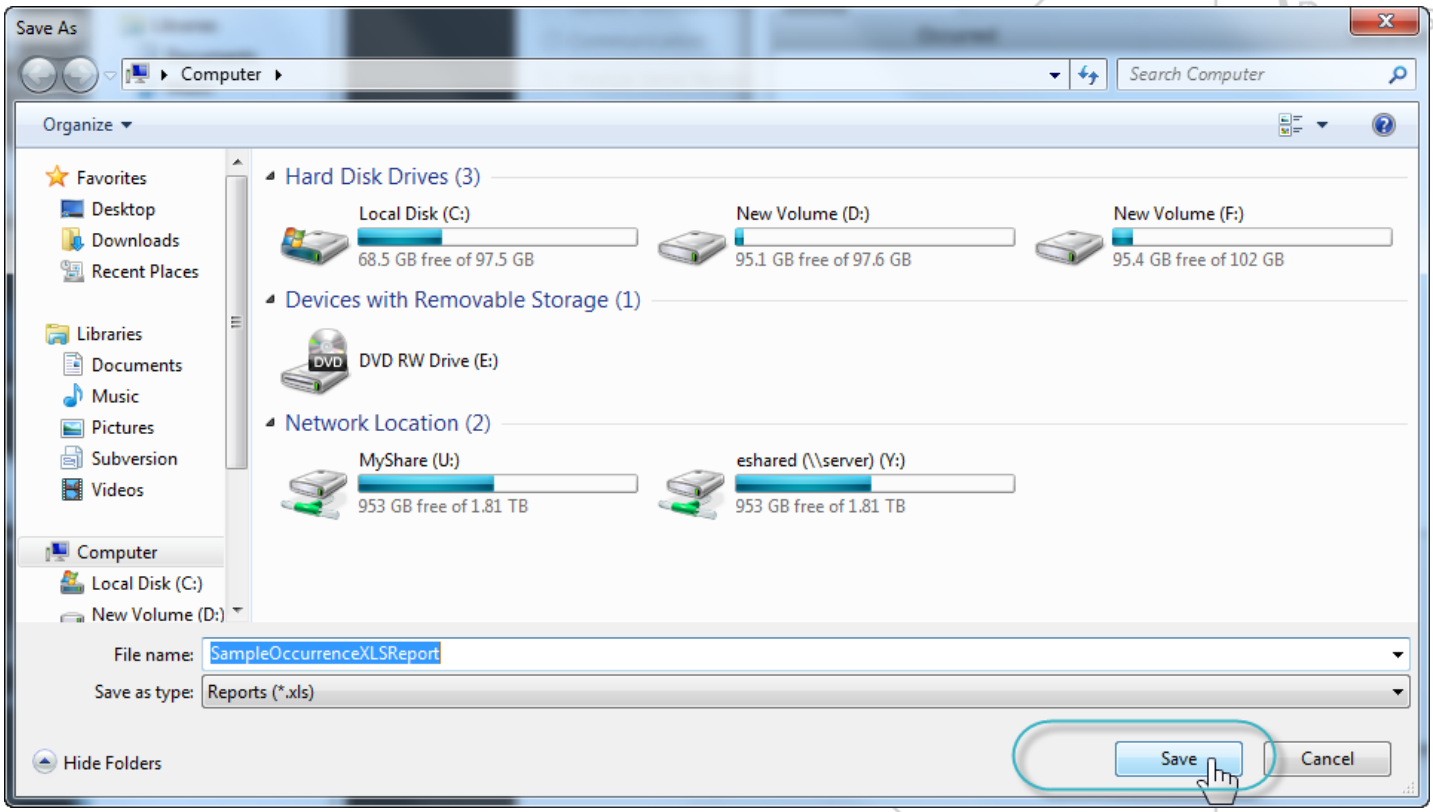
2. The **Save As** dialog box is displayed. In the **File Name** drop-down box, type-in the Excel file name.



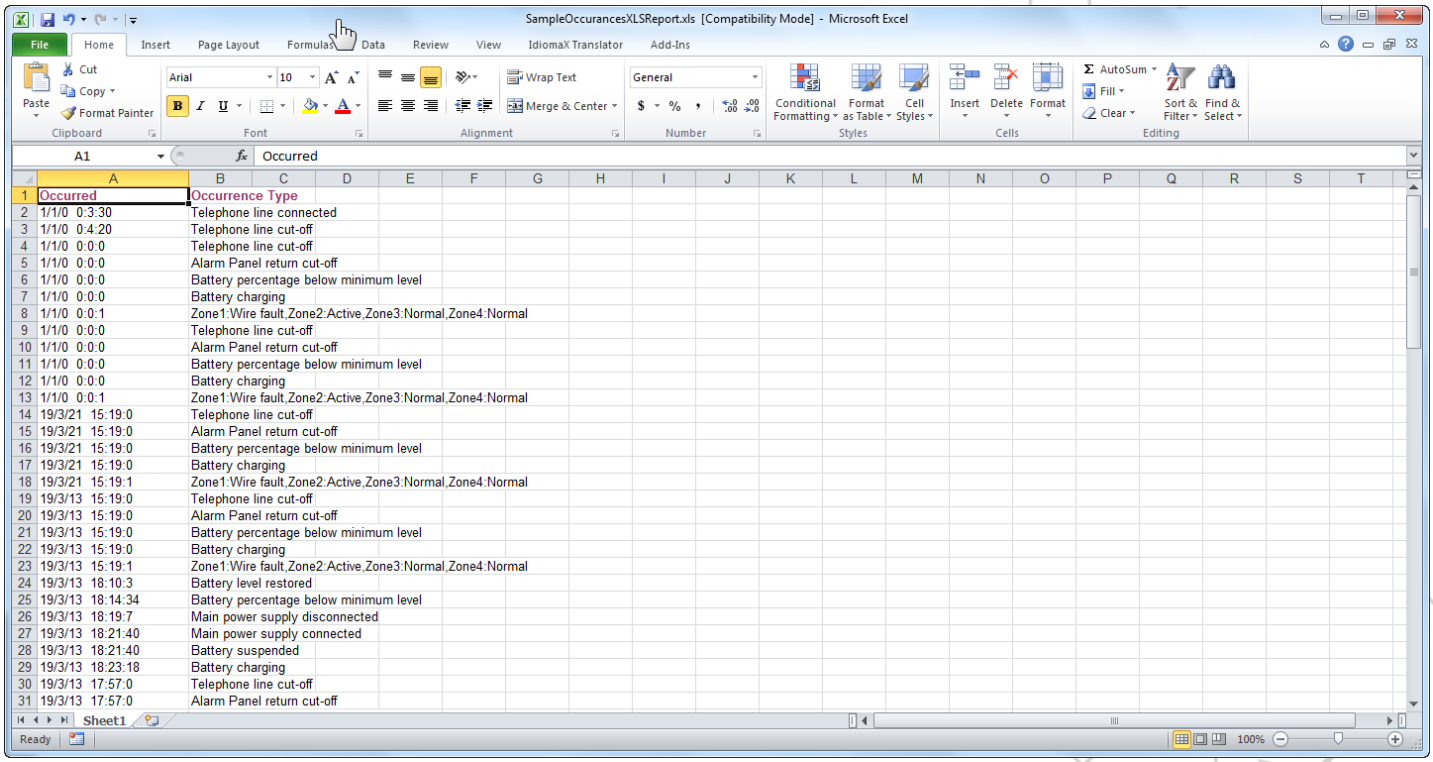
3. Select a location in your hard disk drive where you want to save the Excel file.



4. Click the **Save** button.



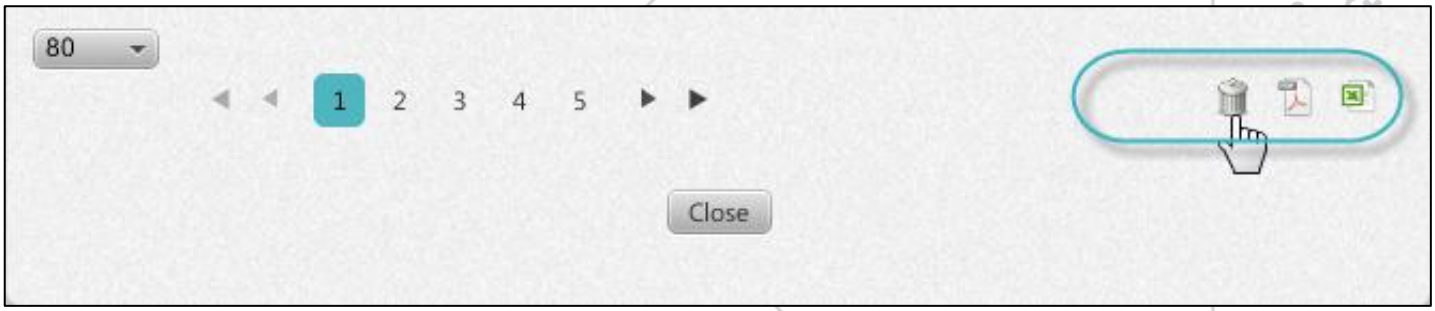
The Event logs in the Excel format are generated and saved in the specified location in your hard drive. A sample Event logs Excel file is shown below.



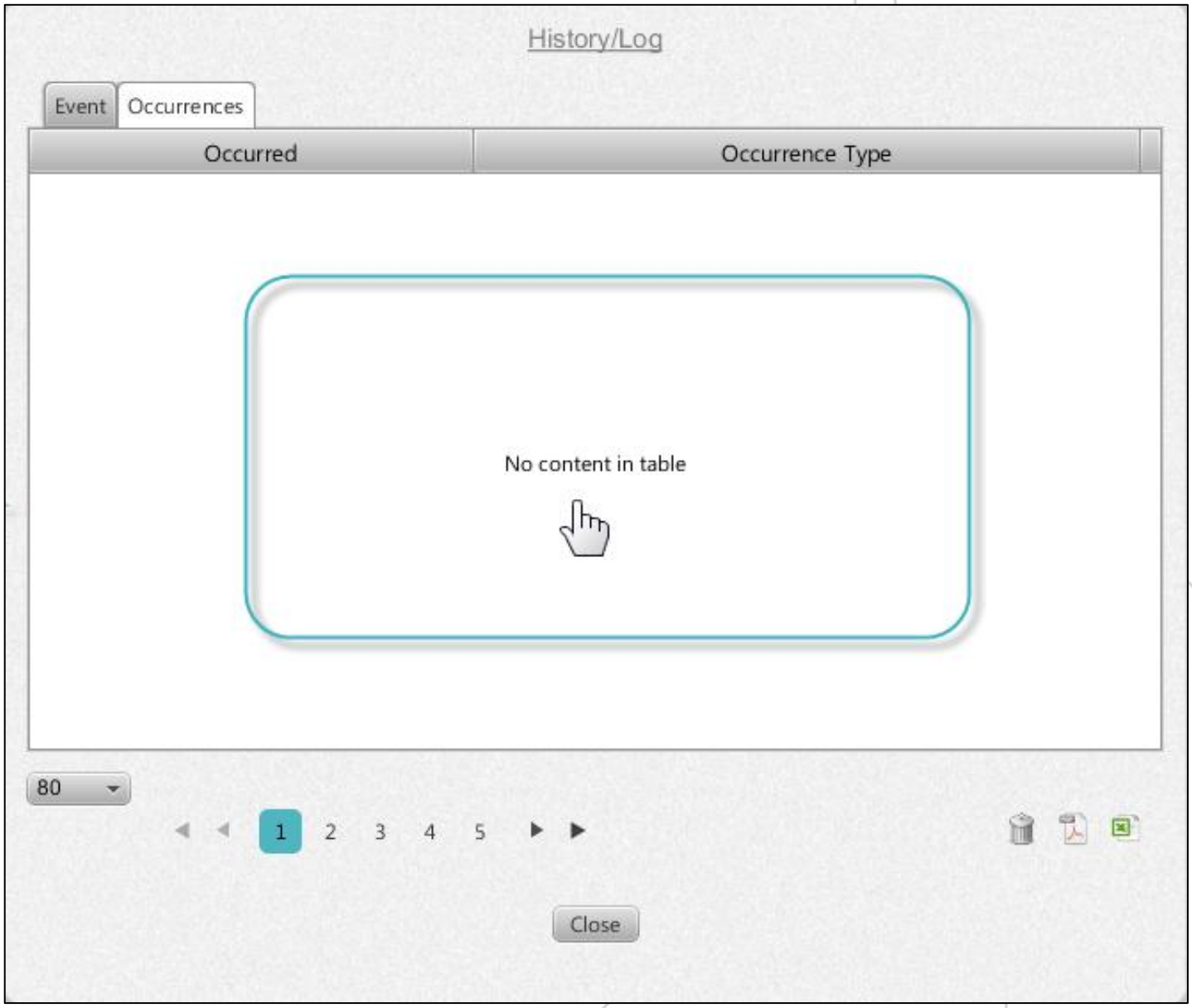
16.2.4. Delete Event Logs

To delete event logs

1. Click the **Delete**  icon.

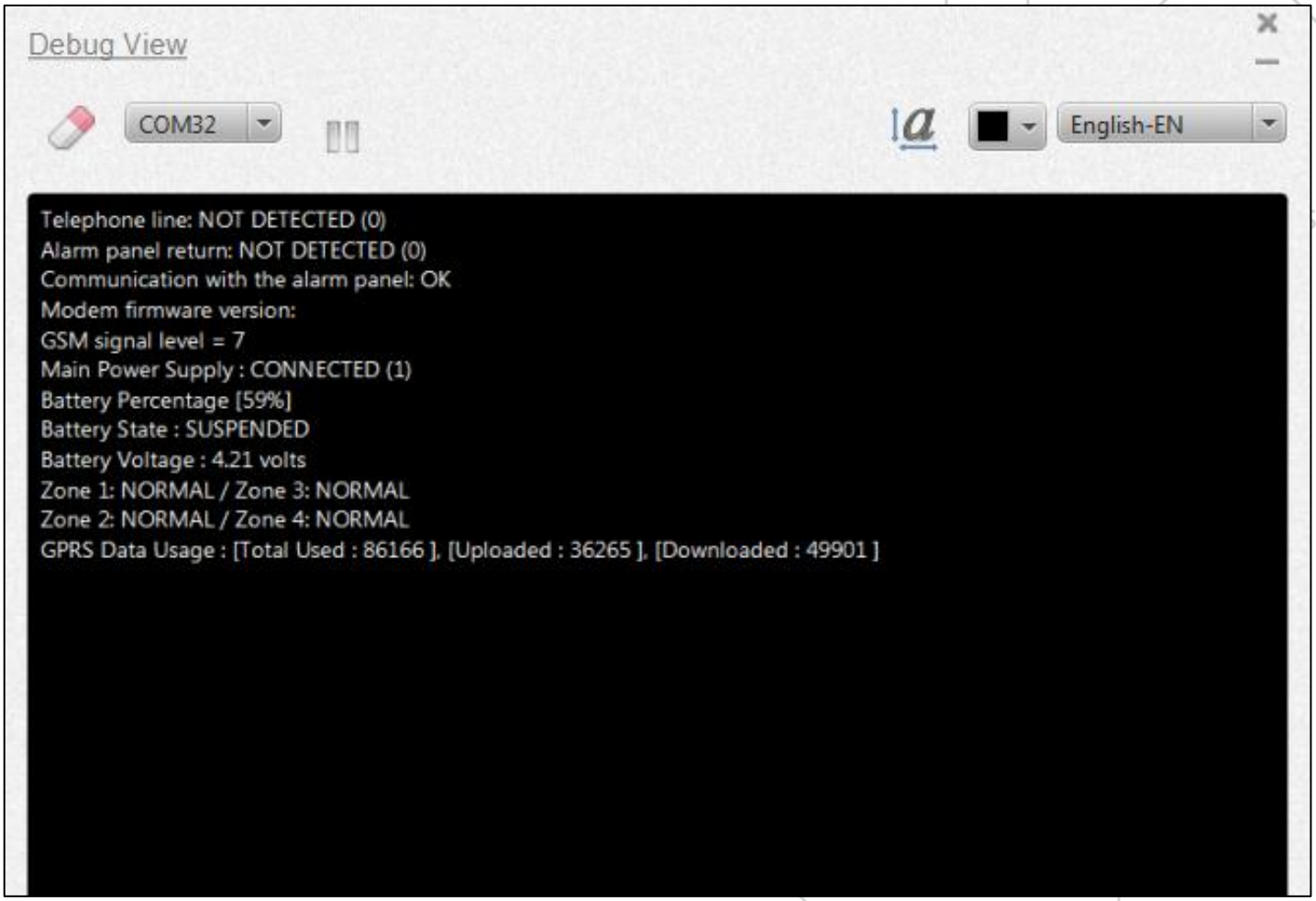


All the Event logs are deleted.


History/Log
Event
Occurrences
Occurred
Occurrence Type
No content in table
80
1
2
3
4
5
Close

17 Debug View

The **Debug View** screen is an inbuilt terminal emulator that displays debug messages related to Pegasus™ NX. The screen allows you to connect/disconnect Debug View, modify the background screen color, modify fonts, change the Debug View language, and clear the Debug View screen by deleting the debug messages.

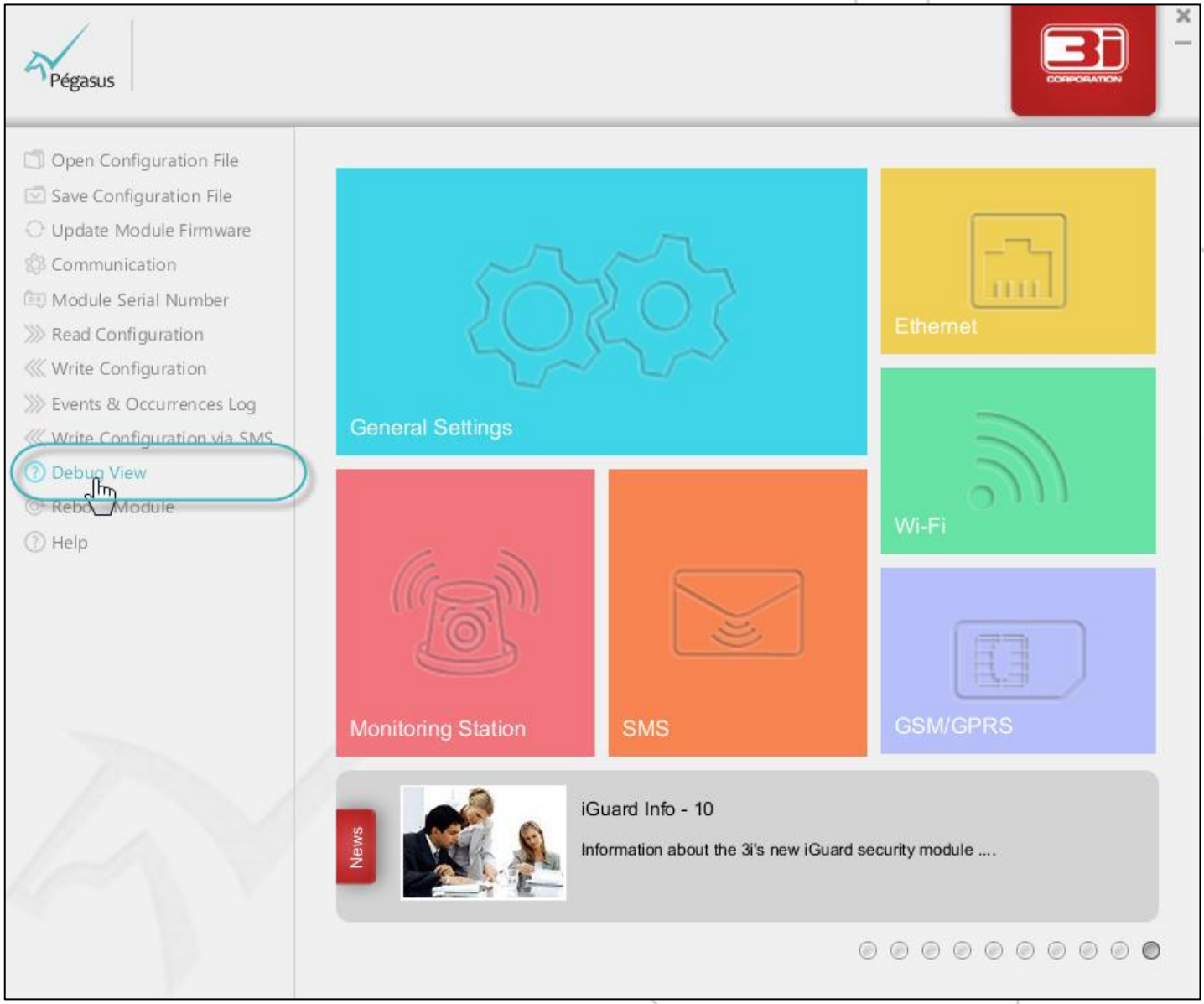


17.1. Manage Debug View

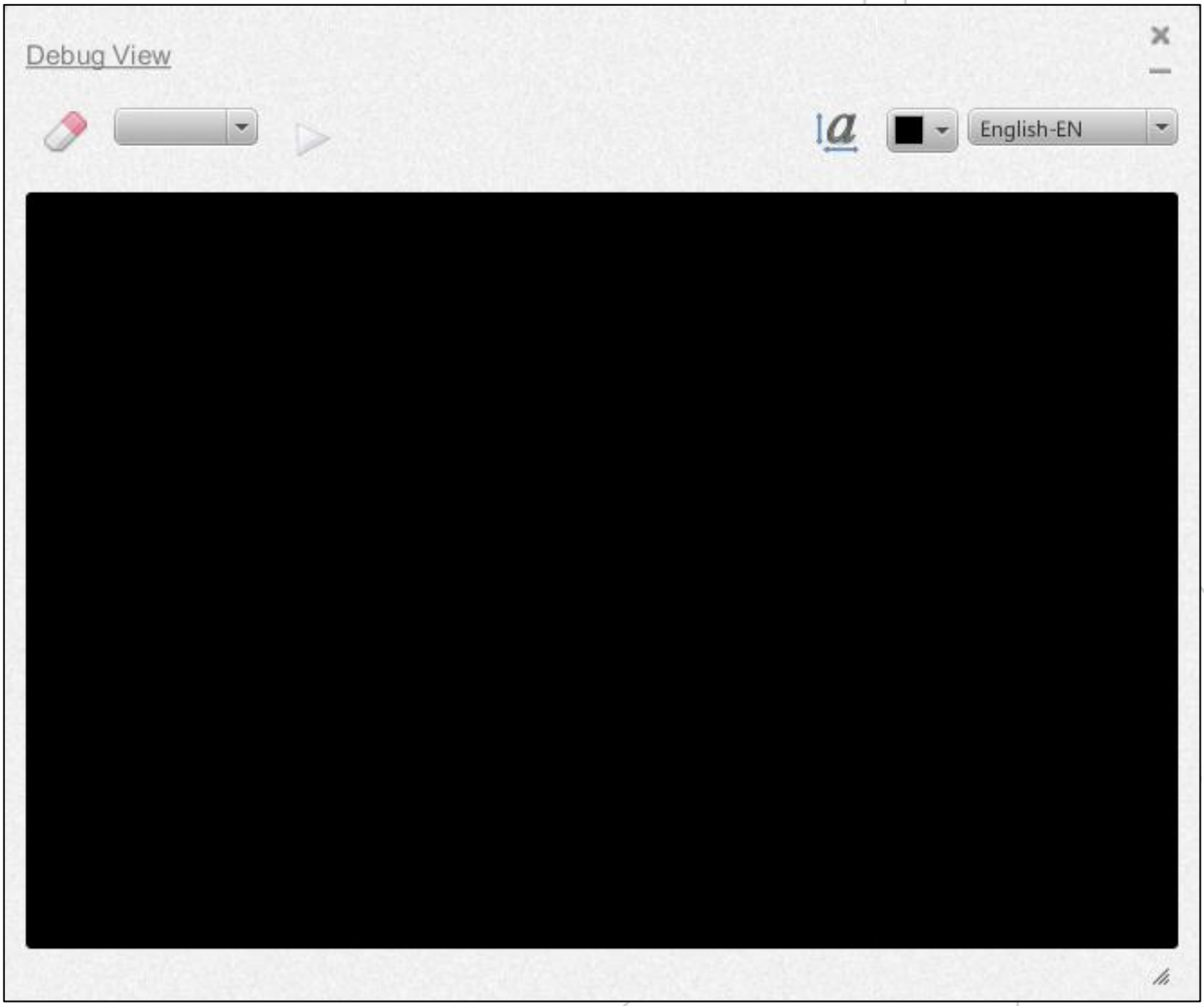
17.1.1. Connect/Disconnect Debug View

To connect debug view

1. On the **Pegasus™ Studio** menu, click **Debug View**.

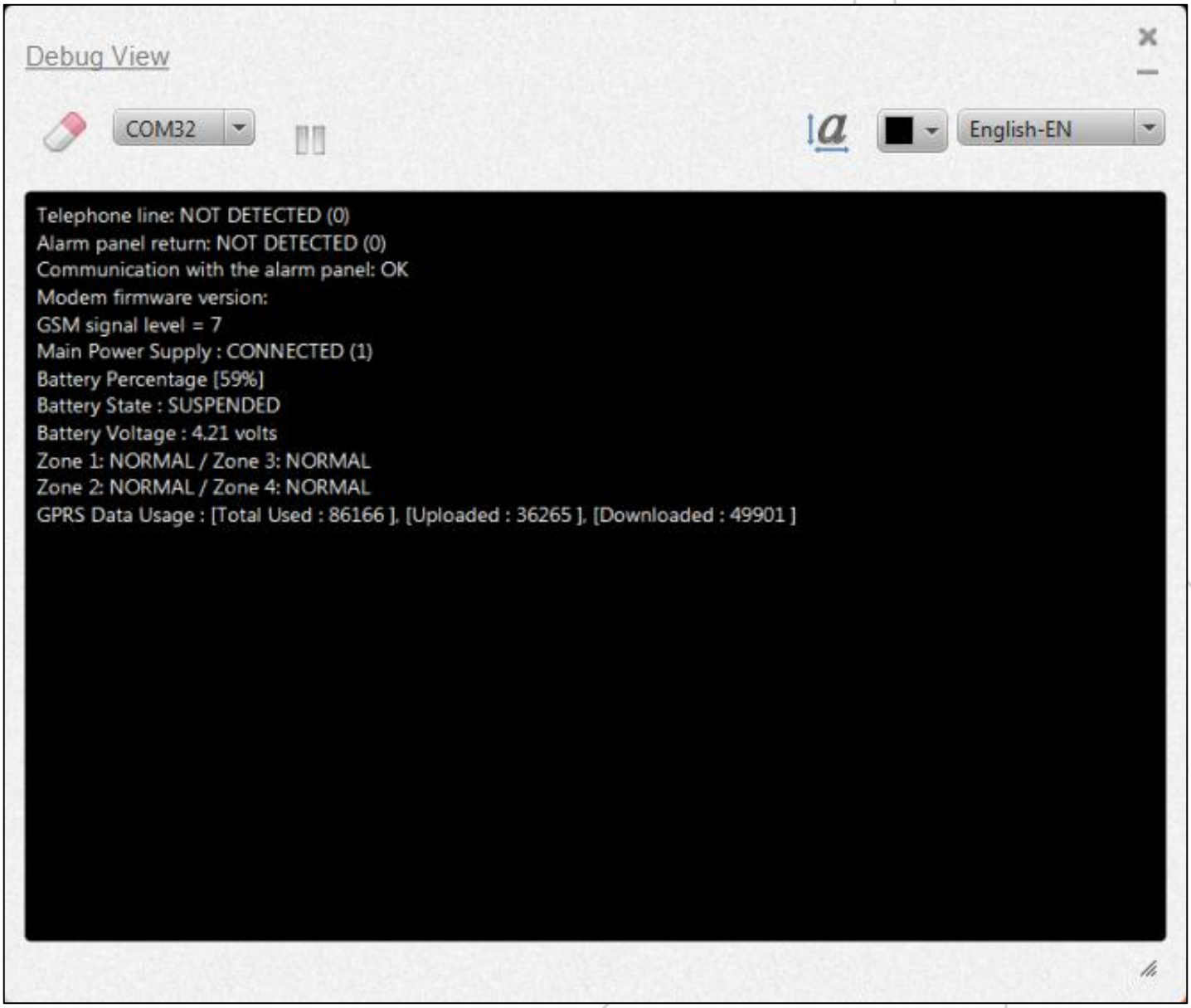


The **Debug View** screen is displayed.



2. Click the **Connect**  icon.

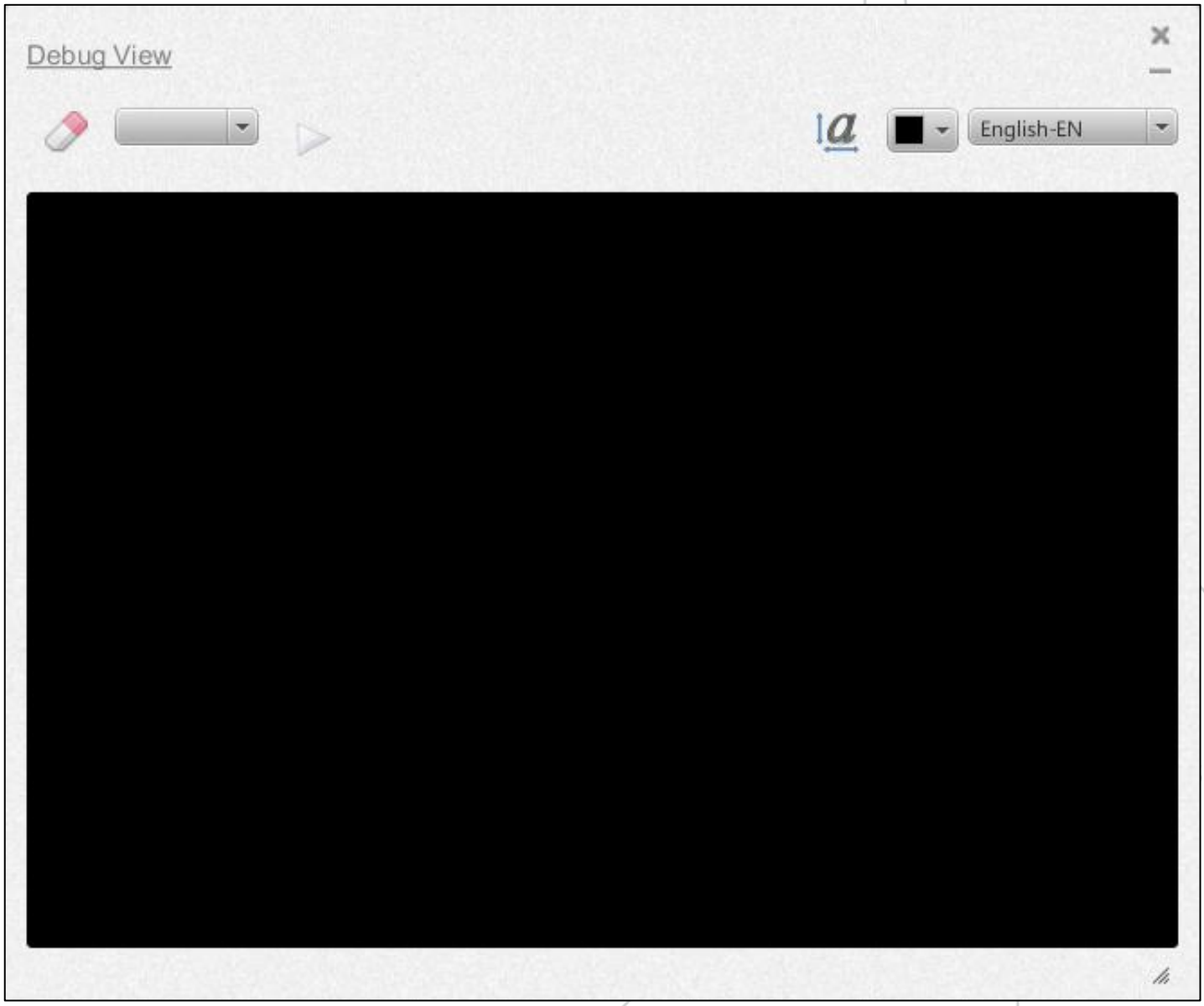
The debug view is connected and the debug messages are displayed in the screen.



To disconnect debug view

1. Click the **Disconnect**  icon.

   The **Debug View** screen is turned blank and all debug messages are disappeared.

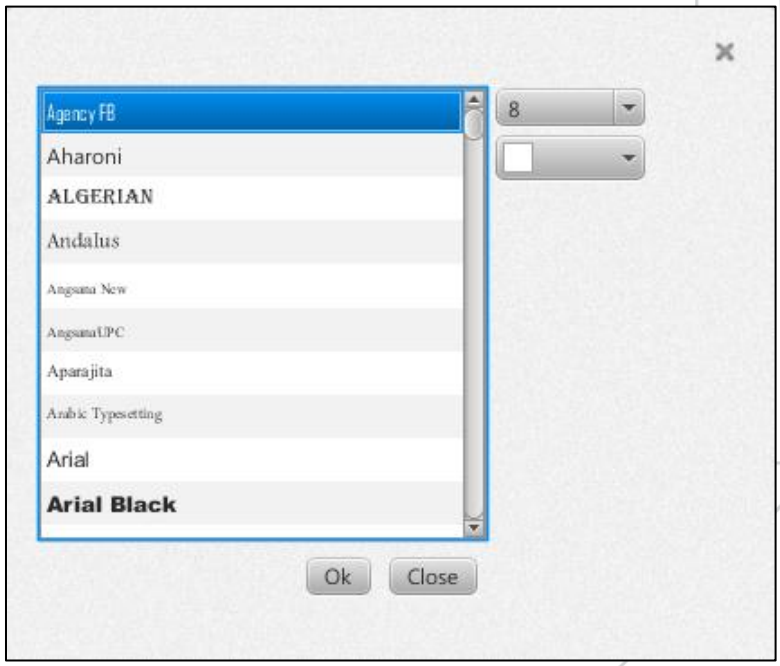


17.1.2. Modify Fonts

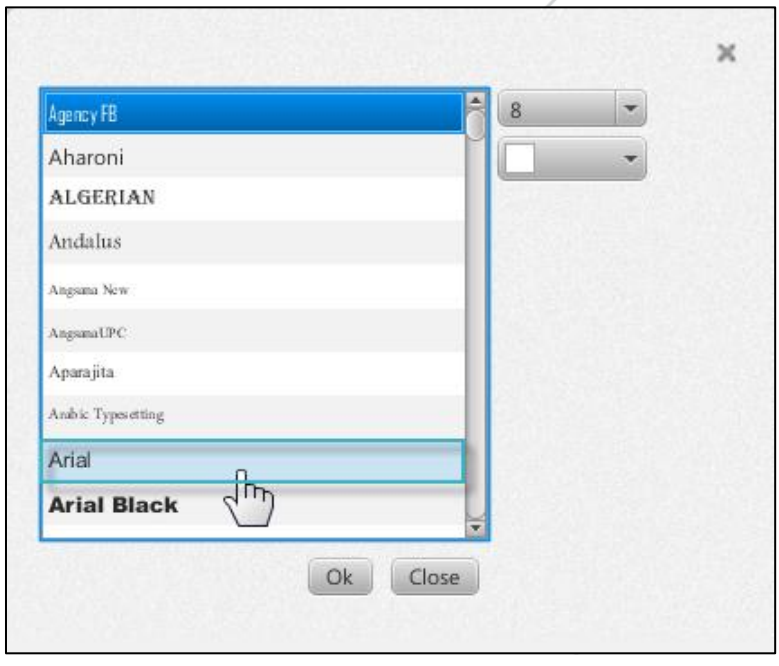
To modify fonts

1. On the **Debug View** screen, click the **Font Selection**  icon.

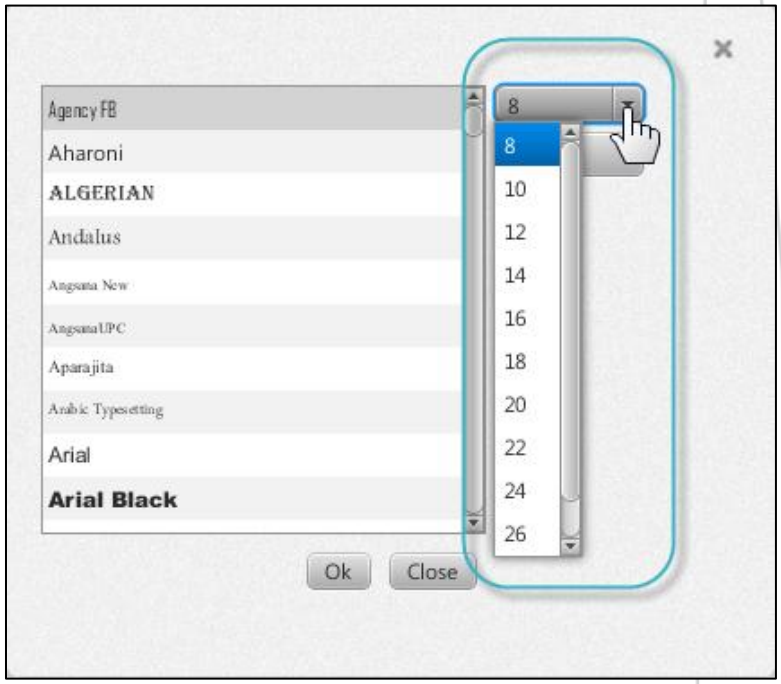
The **Font Selection** dialog box is displayed



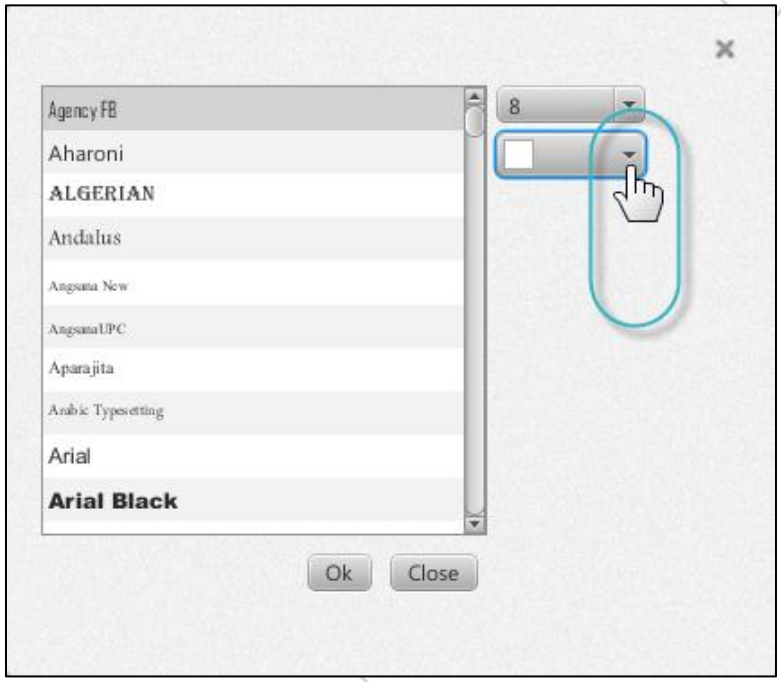
2. Select the **Font Type**.



3. Select the **Font Size.**

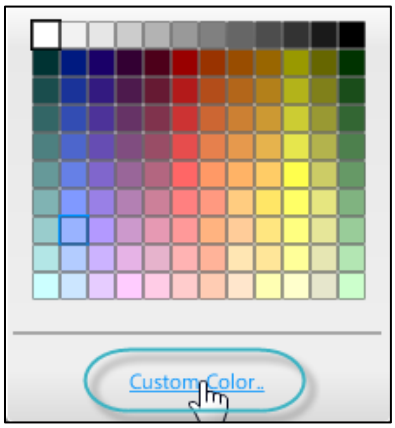


4. To select font color, click the **Font Color** drop-down arrow.

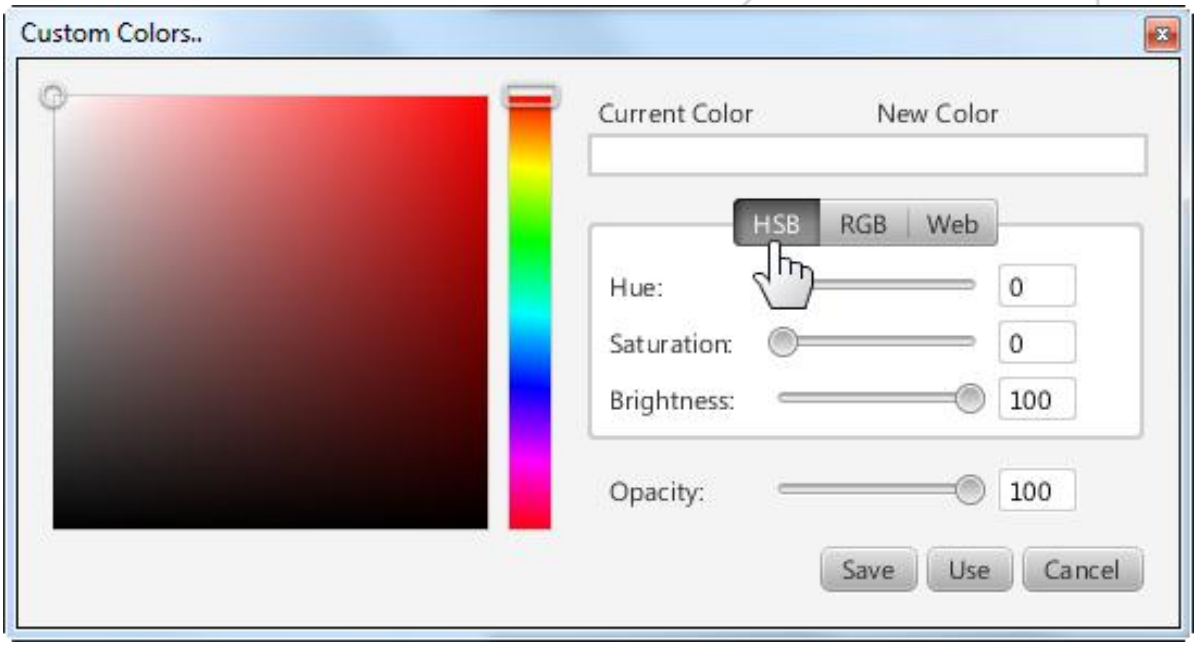


5. The **Color Picker** screen is displayed. To select the font color, click the desired color.

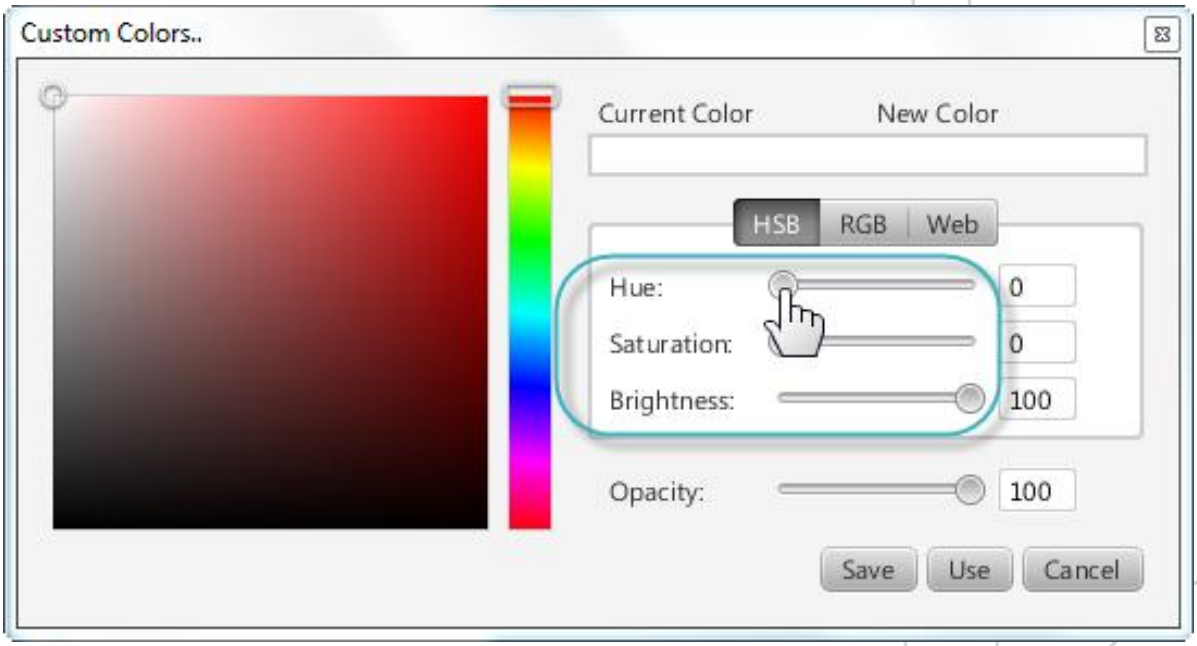
6. To use custom font color, click **Custom Color**.



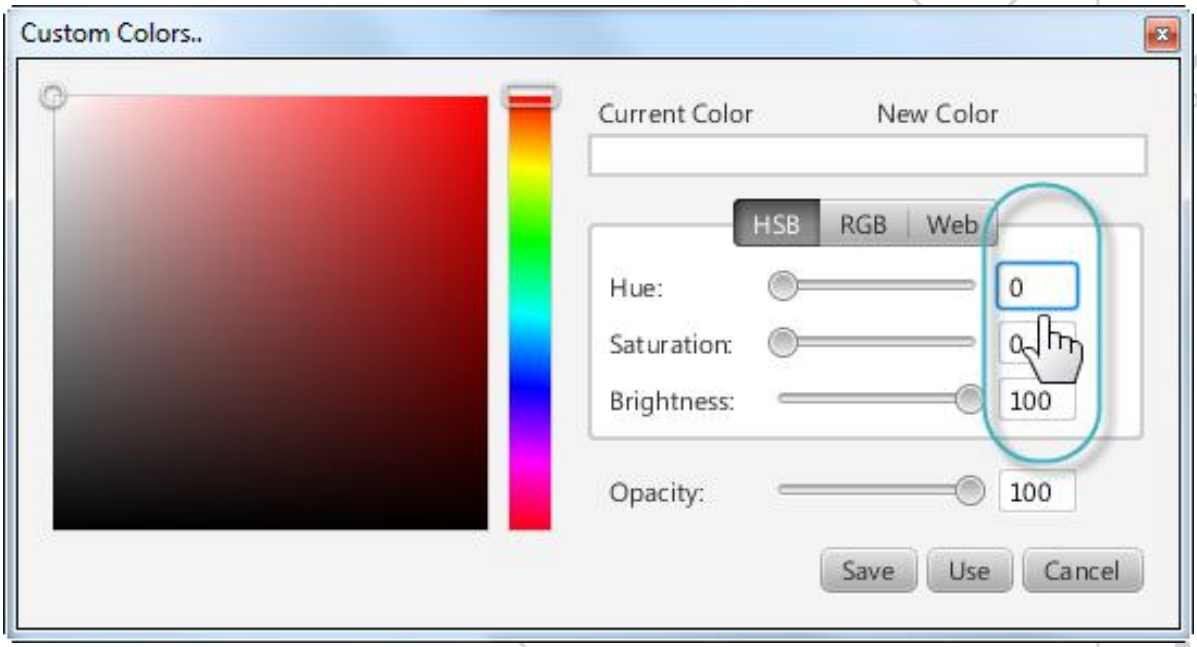
7. The **Custom Colors** dialog box is displayed as shown below. To select font color in HSB mode, click the **HSB** tab.



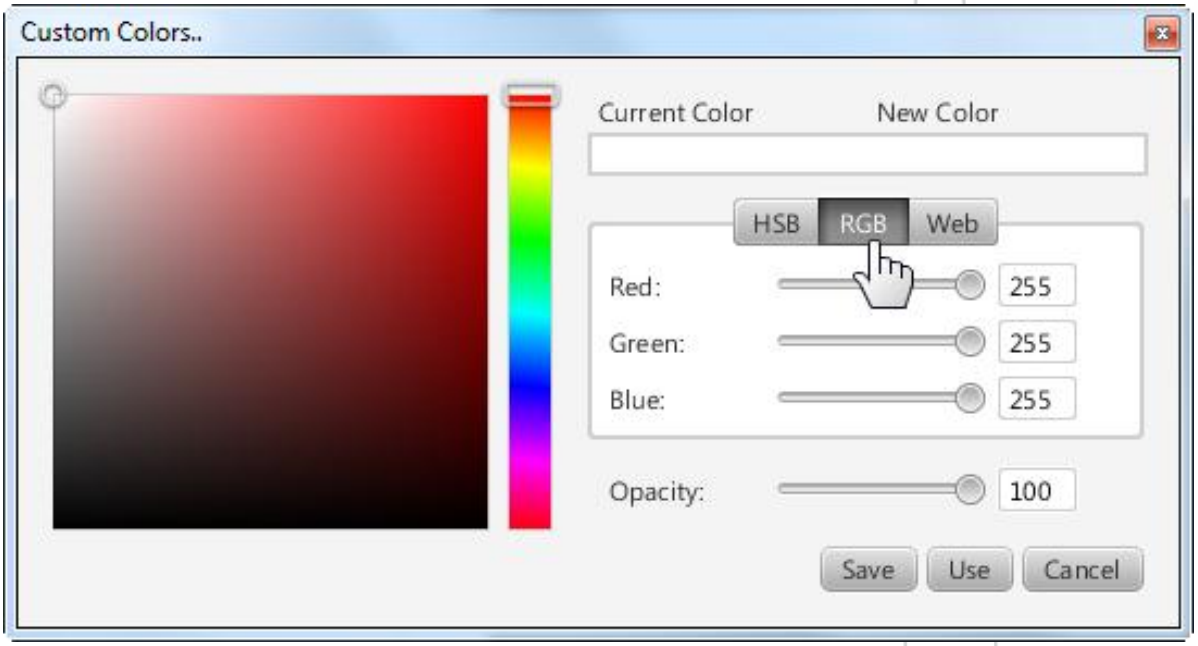
8. Adjust Hue, Saturation and Brightness by using the respective adjustment bar.



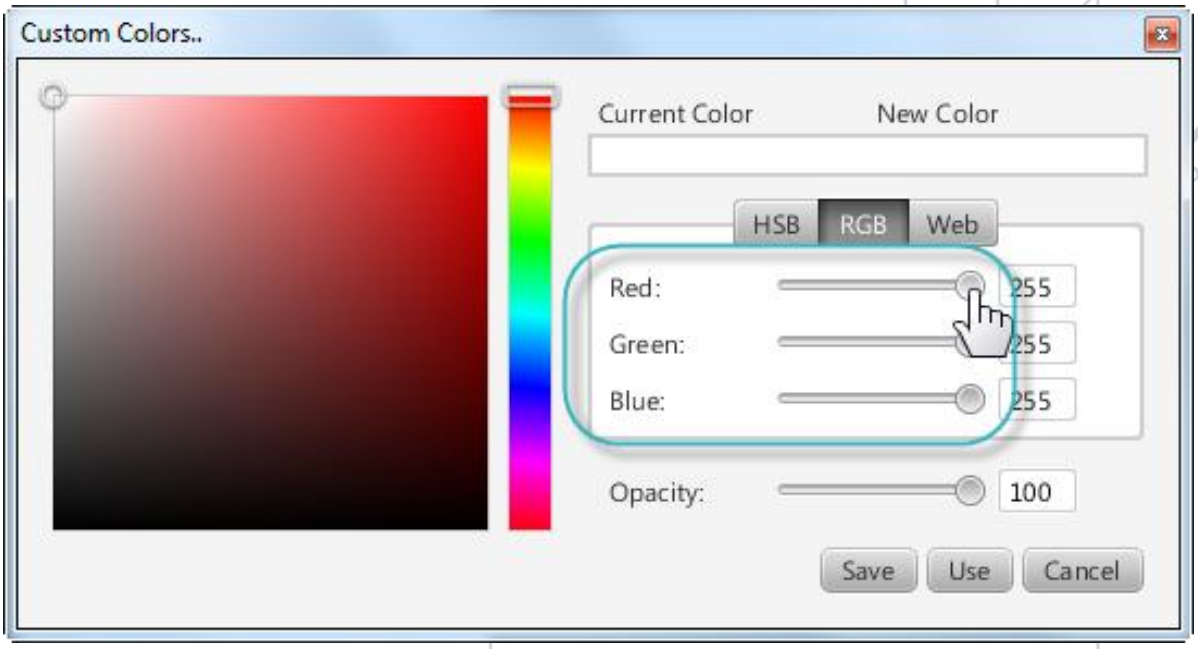
9. If you know the Hue, Saturation and Brightness color codes, type-in the color codes in the respective text boxes.



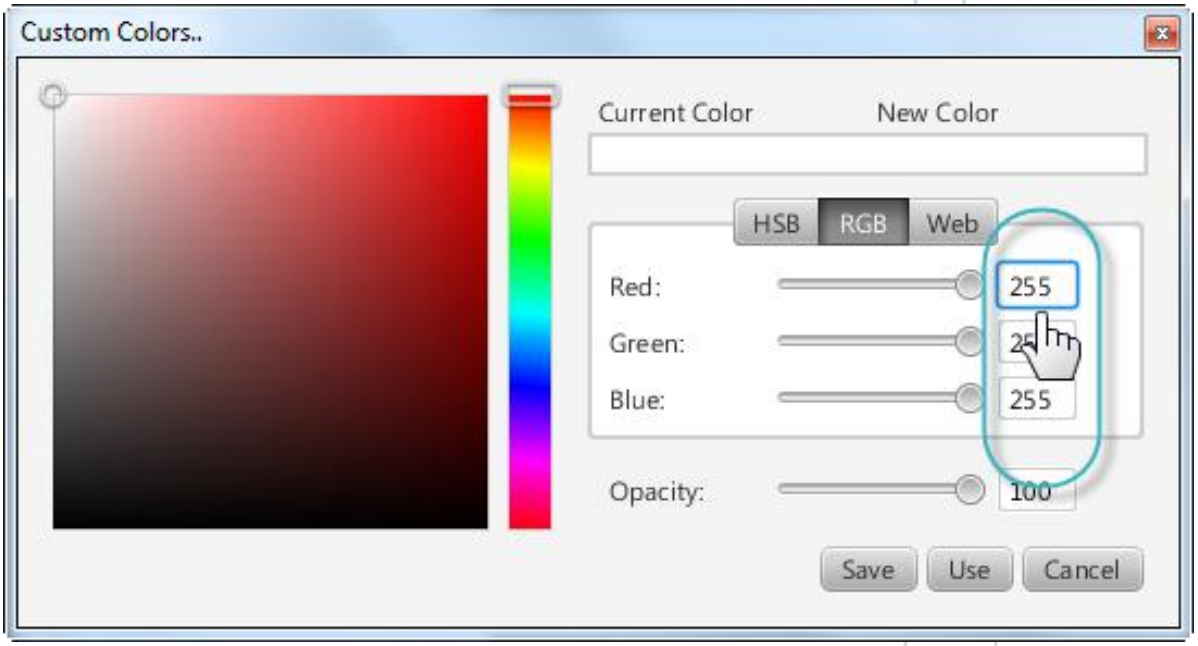
10. To select font color in RGB mode, click the **RGB** tab.



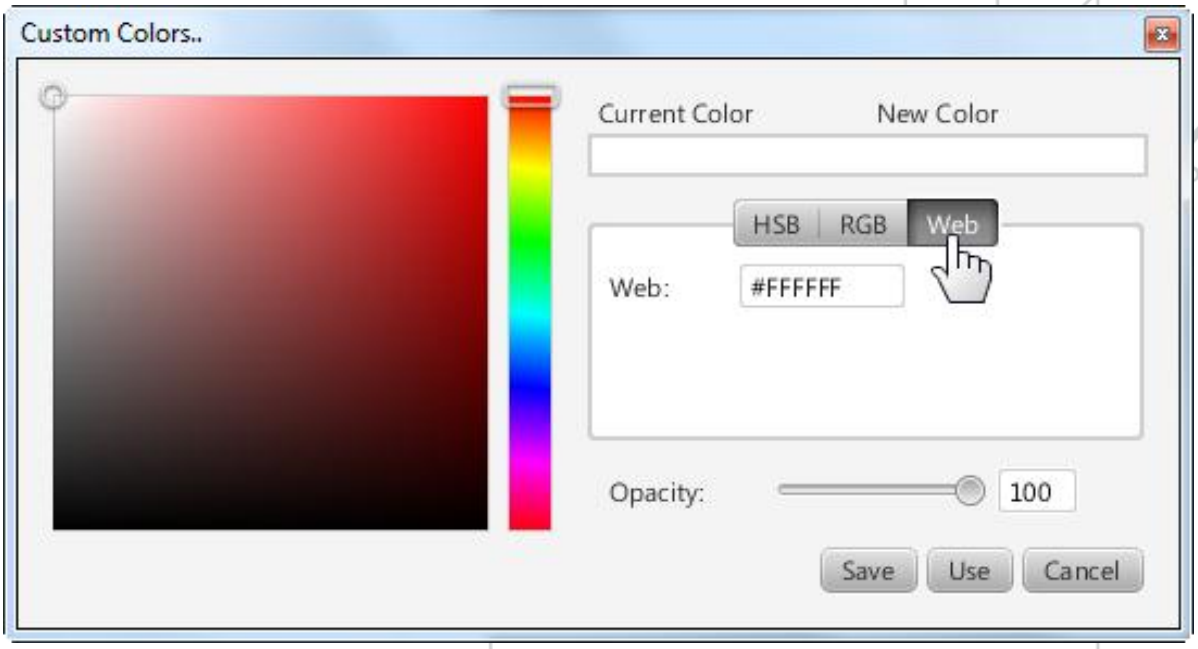
11. Adjust the Red, Green and Blue color codes by using the respective adjustment bar.



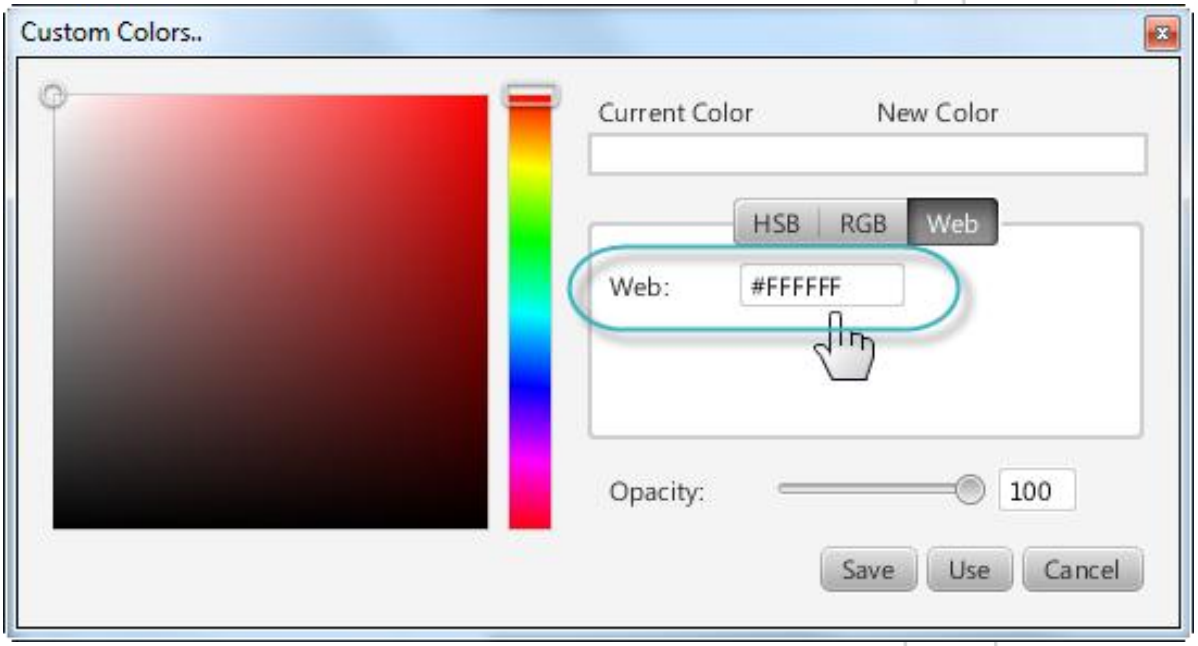
12. If you know the Red, Green and Blue color codes, type-in the color codes in the respective text boxes.



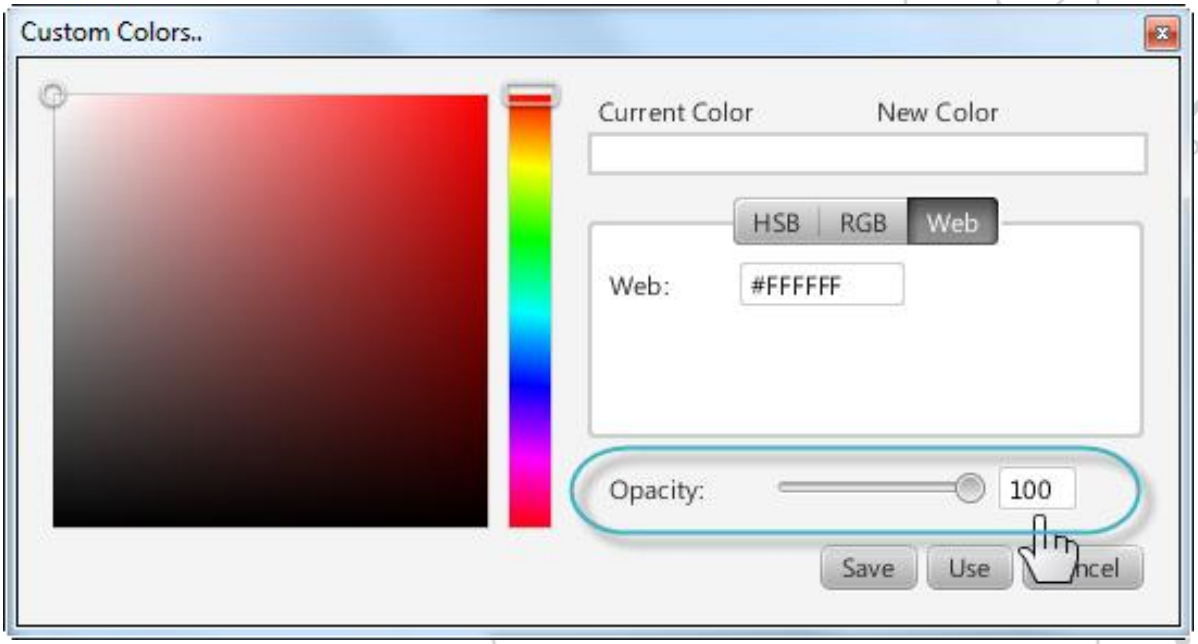
13. To select font color in Web mode, click the **Web** tab.



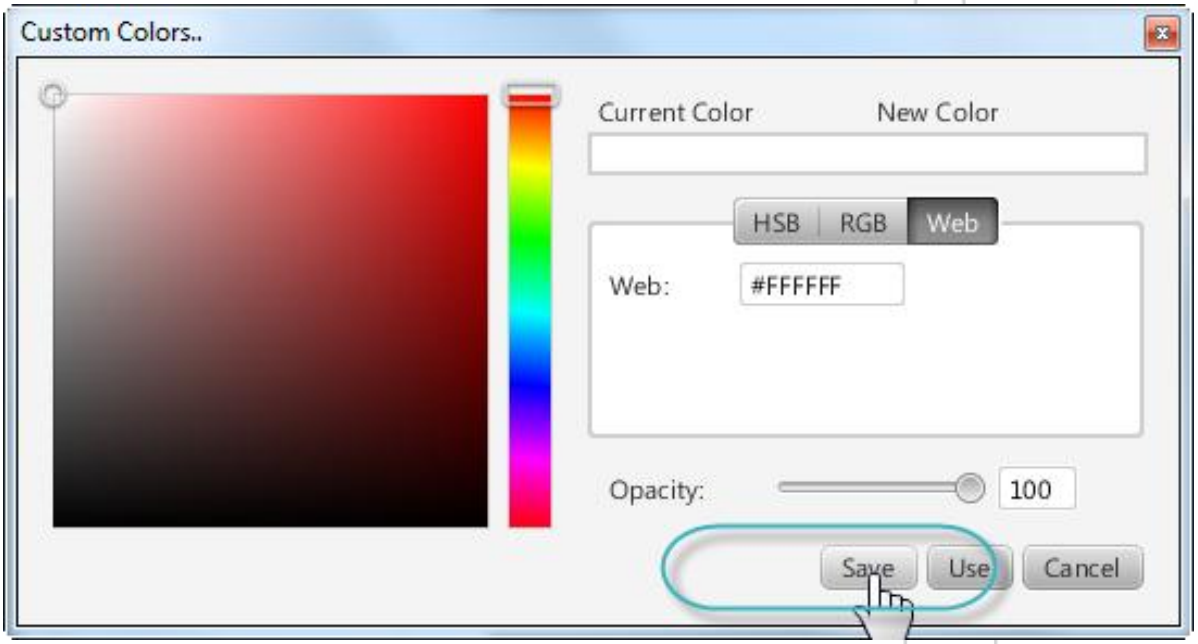
14. In the Web text box, type-in the font color code.



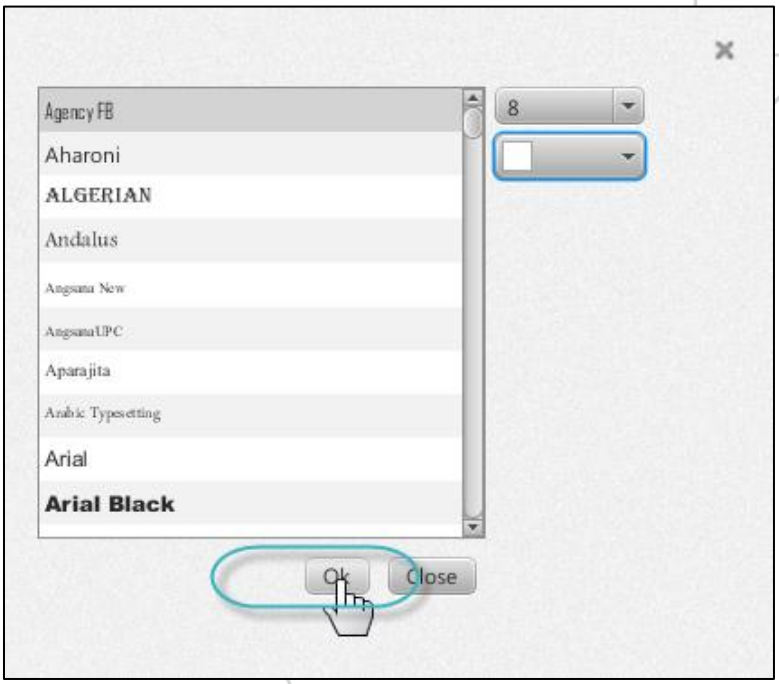
15. To adjust opacity, use the adjustment bar or type-in the opacity value in the text box as shown in the below image.



16. To save the customized color settings, click the **Save** button.



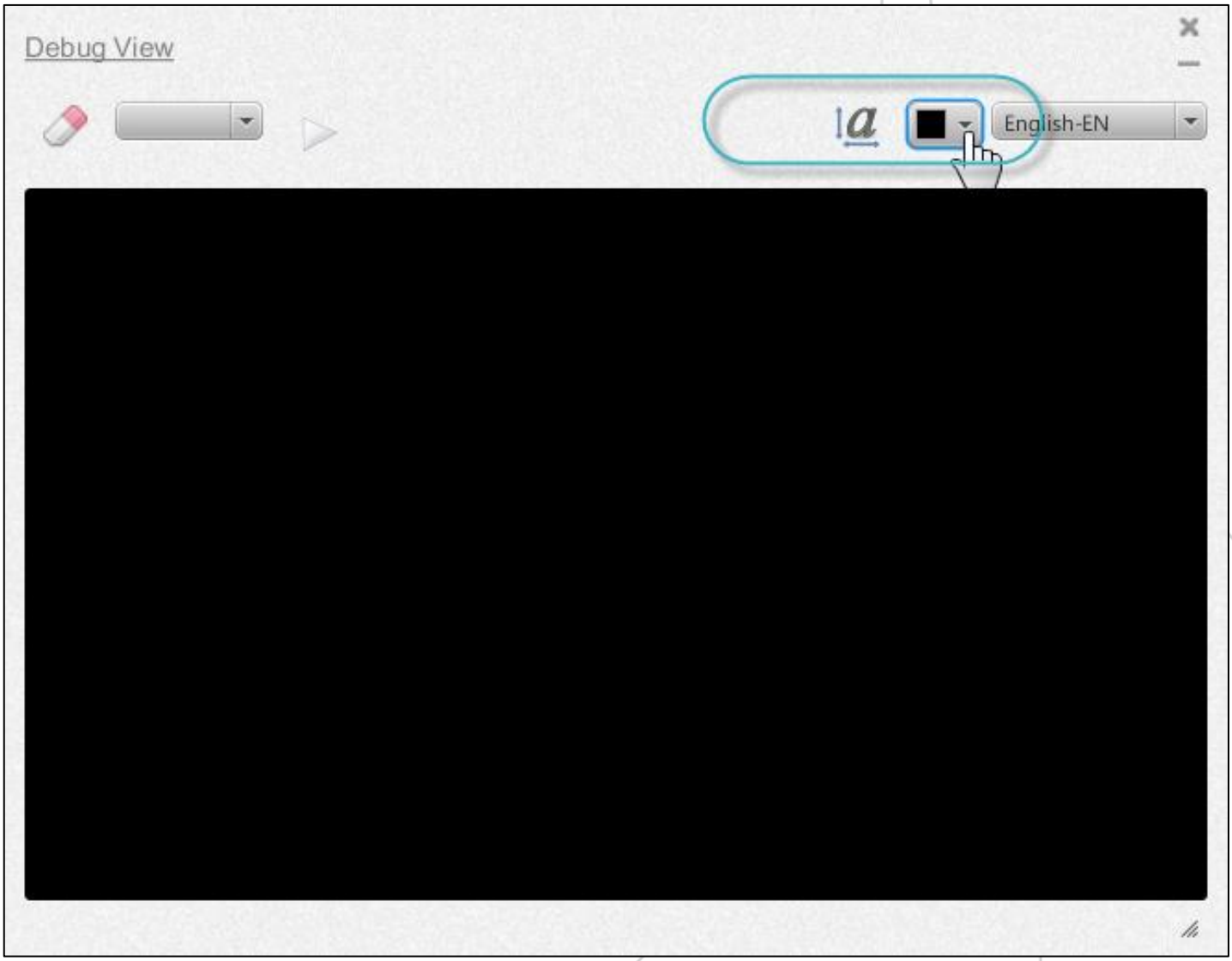
17. To complete the font modification, click the **OK** button.



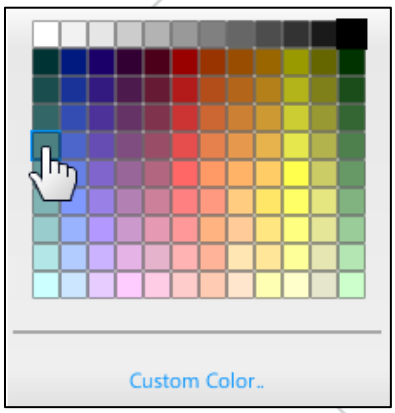
17.1.3. Change the Backgroung Color

To change the backgroung color

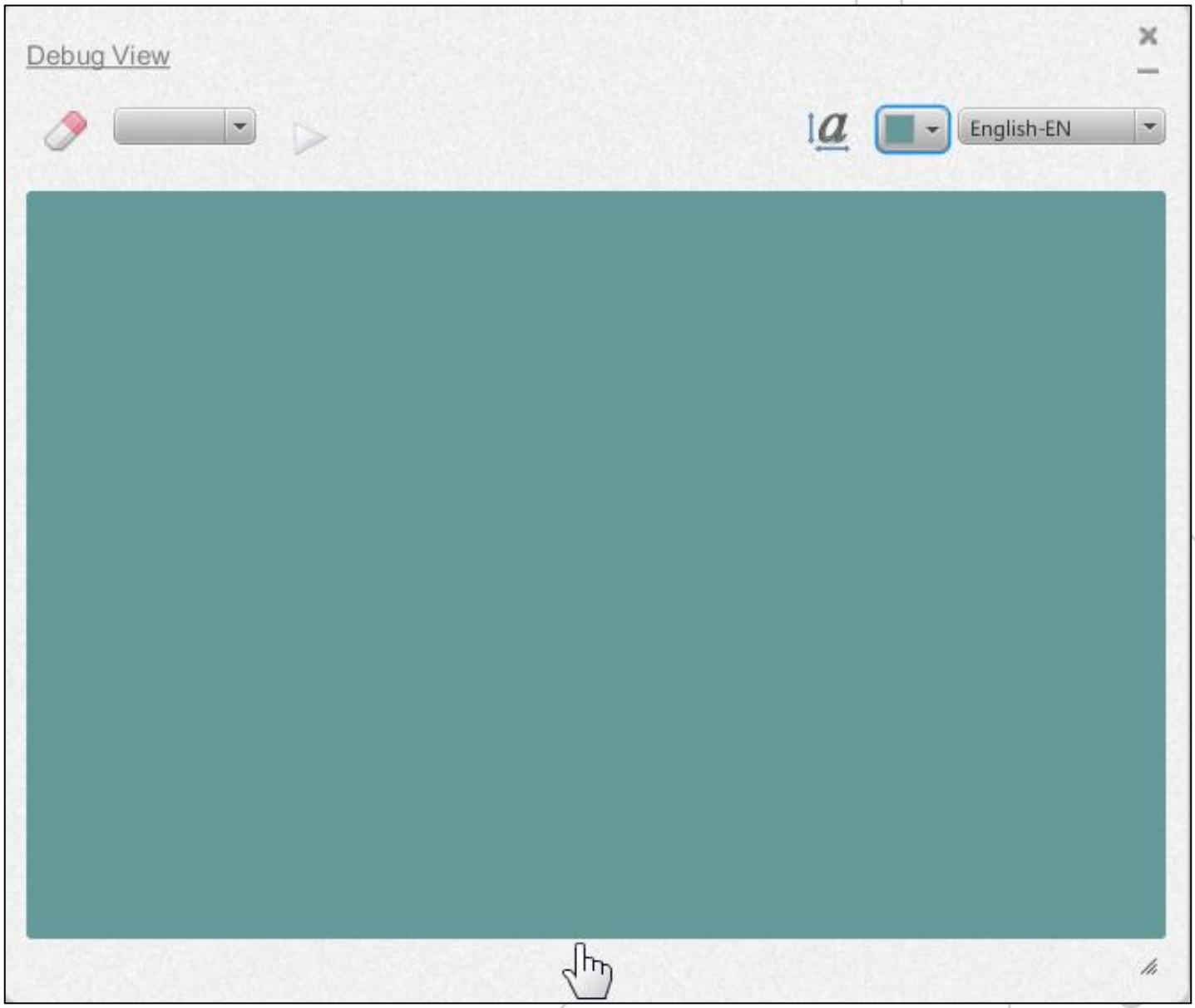
1. Click the drop-down arrow as shown in the below image.



2. The **Color Picker** screen is displayed. Select a background color.



The selected background color is applied as shown below.

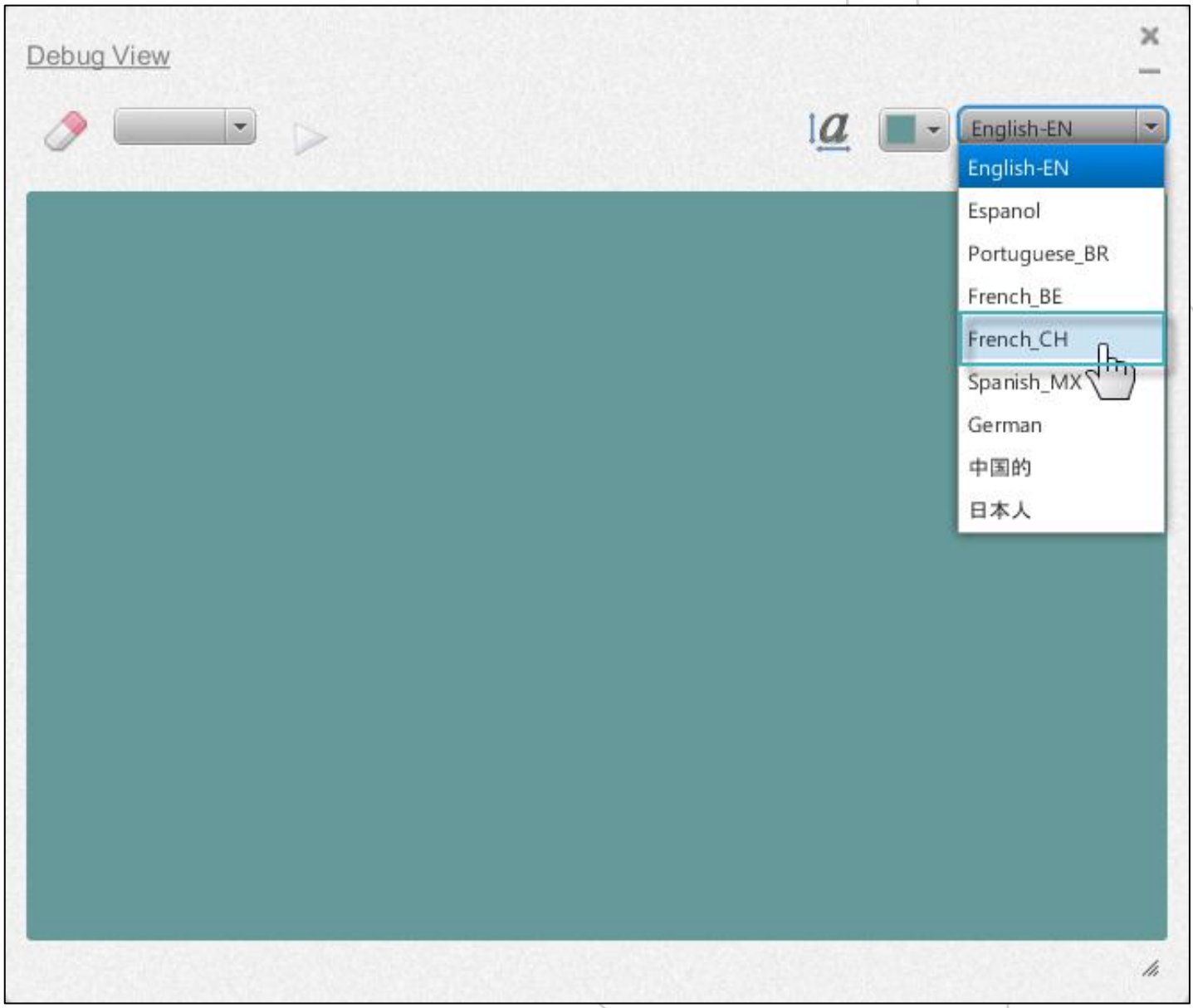


17.1.4. Change the Debug View Language

To change debug view language

1. Click the **Language** drop-down arrow as shown in the below image.

2. On the **Language** menu, select your preferred debug view language.

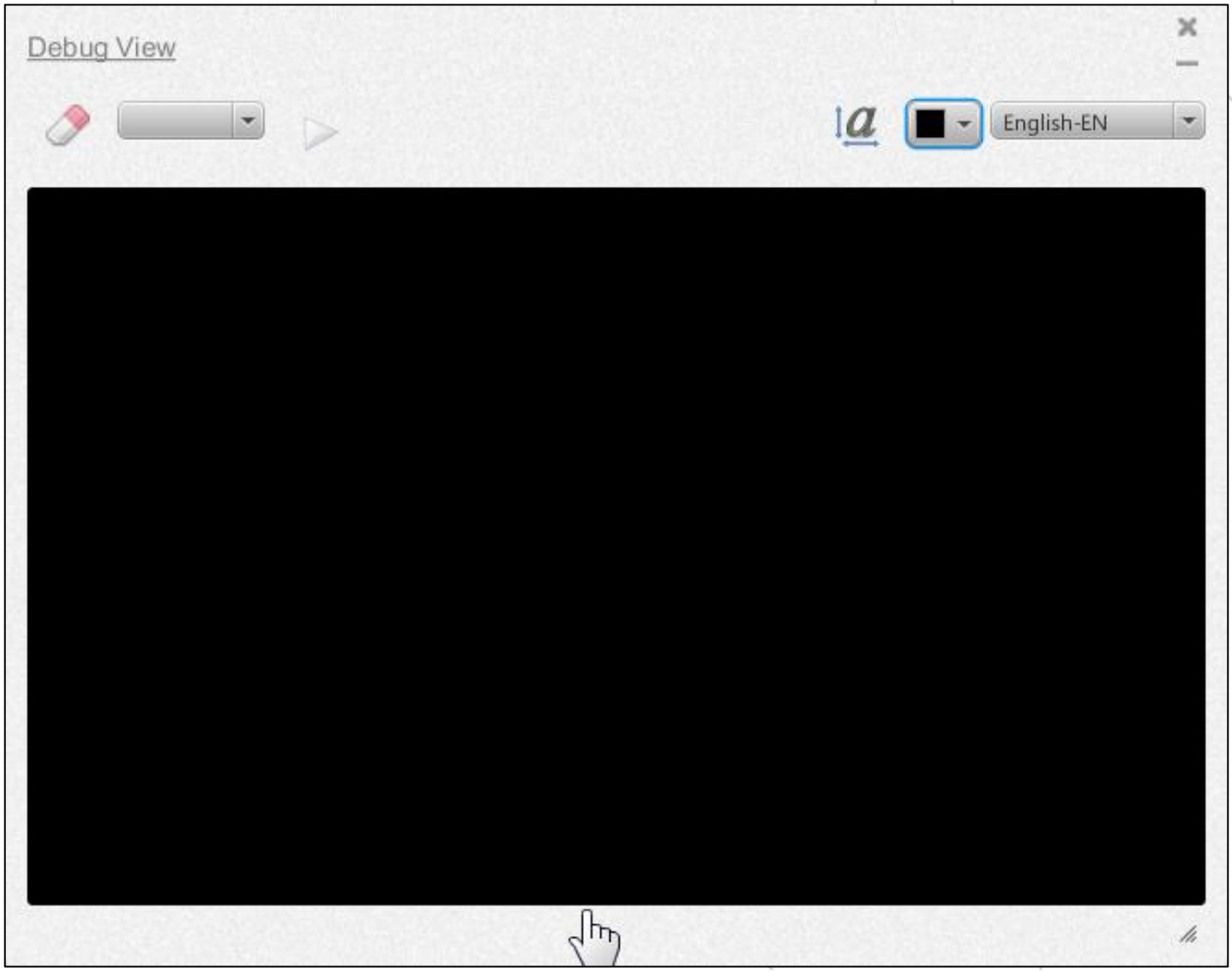


17.1.5. Clear the Debug View Screen

To clear debug view screen

1. Click the **Language** drop-down arrow as shown in the below image.

The Debug View screen is cleared.



18 Appendix

18.1. Abbreviation

GPS	Global Positioning System	SIM	Subscriber Identity Module
GSM	Global System for Mobile Communications	Wi-Fi	Wireless Fidelity
GPRS	General Packet Radio Service	WPA	Wi-Fi Protected Access
DHCP	Dynamic Host Configuration Protocol	WEP	Wired Equivalent Privacy
SMS	Short Message Service	WPA2	Wi-Fi Protected Access version
MMS	Multimedia Messaging Service	SSID	Service Set Identifier
MAC Address	Media Access Control Address	PSK	Phase Shift Keying
IP Address	Internet Protocol Address	AT Command	Attention Command
DNS	Domain Name Service	Device/Module	Pegasus™ NX
Configuration Tool	Pegasus™ Studio		

18.2. Appendix A: GSM Bands

GSM-900 and GSM-1800 are used in most parts of the world: Europe, Middle East, Africa, Australia, Oceania (and most of Asia). In South and Central America the following countries use the following:

- Peru – GSM-1900
- Costa Rica – GSM-1800
- Brazil – GSM-850, 900, 1800 and 1900
- Guatemala – GSM-850, GSM-900 and 1900
- El Salvador – GSM-850, GSM-900 and 1900
- Venezuela – GSM-850, GSM-900 and 1900

GSM-900 uses 890–915 MHz to send information from the mobile station to the base station (uplink) and 935–960 MHz for the other direction (downlink), providing 124 RF channels (channel numbers 1 to 124) spaced at 200 kHz. Duplex spacing of 45 MHz is used. Guard bands 100 kHz wide are placed at either end of the range of frequencies.

GSM-1800

GSM-1800 uses 1,710–1,785 MHz to send information from the mobile station to the base transceiver station (uplink) and 1,805–1,880 MHz for the other direction (downlink), providing 374 channels (channel numbers 512 to 885). Duplex spacing is 95 MHz. GSM-1800 is also called DCS (Digital Cellular Service) in the United Kingdom, while being called PCS in Hong Kong " – not to mix up with GSM-1900 which is commonly called PCS in the rest of the world. Mobile Communication Services on Aircraft (MCA) uses GSM1800.

GSM-850 and GSM-1900

GSM-850 and GSM-1900 are used in Argentina, Brazil, Canada, the United States and many other countries in the Americas.

GSM-850 uses 824–849 MHz to send information from the mobile station to the base station (uplink) and 869–894 MHz for the other direction (downlink). Channel numbers are 128 to 251.

GSM-850 is also sometimes called GSM-800 because this frequency range was known as the "800 MHz band" (for simplification) when it was first allocated for AMPS in the United States in 1983.

The term Cellular is sometimes used to describe the 850 MHz band, because the original analog cellular mobile communication system was allocated in this spectrum.

GSM-1900 uses 1,850–1,910 MHz to send information from the mobile station to the base station (uplink) and 1,930–1,990 MHz for the other direction (downlink). Channel numbers are 512 to 810.

PCS is the original name in North America for the 1,900 MHz band. It is an initialism for Personal Communications Service.

18.3. Appendix B: AT Commands

AT commands are used to control MODEMs. AT is the abbreviation for Attention. These commands come from Hayes commands that were used by the Hayes smart modems. The Hayes commands started with AT to indicate the attention from the MODEM. The dial up and wireless MODEMs (devices that involve machine to machine communication) need AT commands to interact with a computer. These include the Hayes command set as a subset, along with other extended AT commands.

AT commands with a GSM/GPRS MODEM or mobile phone can be used to access following information and services: Information and configuration pertaining to mobile device or MODEM and SIM card, SMS services, MMS services, Fax services, and data and voice link over mobile network.

The Hayes subset commands are called the basic commands and the commands specific to a GSM network are called extended AT commands.

18.4. Appendix C: Dynamic Host Configuration Protocol

DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many ISPs use dynamic IP addressing for dial-up users.

18.5. Appendix D: Media Access Control Address

MAC address is a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sub-layers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network medium. Consequently, each different type of network medium requires a different MAC layer.

18.6. Appendix E: Internet Protocol Address

IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages are based on the IP address of the destination.

The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address.

Within an isolated network, you can assign IP addresses at random as long as each one is unique. However, connecting a private network to the Internet requires registered IP addresses (called Internet addresses) to avoid duplicates.

An IP address can be static or dynamic. A static IP address will never change and it is a permanent Internet address. A dynamic IP address is a temporary address that is assigned each time a computer or device accesses the Internet.

The four numbers in an IP address are used in different ways to identify a particular network and a host on that network. Four regional Internet registries: ARIN, RIPE NCC, LACNIC and APNIC.

18.7. Appendix F: Gateway

Gateway is a node on a network that serves as an entrance to another network. In enterprises, gateway is a computer that routes the traffic from a workstation to the outside network that is serving the Web pages. In homes, the gateway is the ISP that connects the user to the internet.

In enterprises, the gateway node often acts as a proxy module and a firewall. The gateway is also associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch, which provides the actual path for the packet in and out of the gateway.

18.8. Appendix G: Domain Name Service

DNS is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS module doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

18.9. Appendix H: Proxy Module and Proxy Exception

Proxy module is a module that sits between a client application, such as a web browser, and a real module. It intercepts all requests to the real module to see if it can fulfill the requests itself. If not, it forwards the request to the real module.

Proxy modules have two main purposes:

Improve Performance: Proxy modules can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time. Consider the case where both user X and user Y access the World Wide Web through a proxy module. First user X requests a certain Web page, which we'll call Page 1. Sometime later, user Y requests the same page. Instead of forwarding the request to the Web module where Page 1 resides, which can be a time-consuming operation, the proxy module simply returns the Page 1 that it already fetched for user X. Since the proxy module is often on the same network as the user, this is a much faster operation.

Filter Requests: Proxy modules can also be used to filter requests.

Proxy Exception

In Pegasus™, some network requests need to bypass the proxy module. The most common reason to bypass the proxy is for local/intranet addresses.

18.10. Appendix I: Service Set Identifier (SSID)

SSID is a case sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent over a wireless local-area network (WLAN) that acts as a password when a mobile device tries to connect to the basic service set (BSS) - a component of the IEEE 802.11 WLAN architecture.

SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID to enable effective roaming. As part of the association process, a wireless client must have the same SSID as the one put in the access point or it will not be permitted to join the BSS.

An SSID is also referred to as a *network name* because essentially it is a name that identifies a wireless network.

18.11. Appendix J: Phase Shift Keying

PSK is a modulation technique used by modems in which different phase angles in the carrier signal are used to represent the binary states of 0 and 1.

The simplest method of PSK, also called biphase modulation, uses two signal phases - 0 degrees and 180 degrees. The digital signal is broken up according to time into binary digits and the state (1 or 0) of each bit is determined according

the state of the bit that preceded it. If the phase of the bit does not change then the state of the signals stays the same. If the phase of the signal changes by 180 degrees, then the signal state changes (from 0 to 1, or 1 to 0).

There are more complex forms of PSK that rely on four or eight phases to transmit data at a faster rate.

18.12. Appendix K: Wireless Security Protocol: WEP, WPA and WPA2

Various wireless security protocols are developed to protect home wireless networks. These wireless security protocols include WEP, WPA, and WPA2. In addition to preventing uninvited guests from connecting to your wireless network, wireless security protocols encrypt your private data as it is being transmitted over the airwaves.

Following are the descriptions of the WEP, WPA, and WPA2 wireless security protocols:

Wired Equivalent Privacy (WEP): The original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks.

Wi-Fi Protected Access (WPA): Introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. Most current WPA implementations use a preshared key (PSK), commonly referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP, pronounced tee-kip) for encryption. WPA uses an authentication module to generate keys or certificates.

Wi-Fi Protected Access version 2 (WPA2) Based on the 802.11i wireless security standard, which was finalized in 2004. The most significant enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption. The security provided by AES is sufficient and approved for use by the U.S. government to encrypt information classified as top secret.